Octoper 2011
Issue 19

Magazine NetworkSet

First Arabic Magazine For Networks



الإعلام القذر

كنت غافلا ضائعا تائها , هذه هي الكلمات التى وصفت نفسي بها عندما كنت من متتبعي التلفاز والأعلام العربي , والحمد لله صحوت من هذه الغفلة لأكتشف عالم قذر يضع أوسخ ماليده ويستورد أوسخ ماليديهم ليجعلوا منا لعبة في أيديهم القذرة , وماصحاني حقيقة هو ربيع الثورات العربية وكيفية تعاطي الأعلام مع كل ثورة فمن كنا نظنهم أفضل السيئين تبين أنهم أسوء السيئين ومن كنا نظنهم أسوء السيئين أكيد لم يتيبن أنهم أفضل السيئين بل أقذر السيئين وخصوصا أن لكل واحد منهم أهدافه القذرة من تسيس العقول وتضيعها وأدخالها في دوامات فارغة تؤثر على عقله وعقيدته وأفكاره فيما بعد , فلو أخذنا الأقنية الأخبارية منذ بدأ الربيع العربي لتمكنا من تحديد من مع من ومن ضد من فهو محكوم بسياسة صاحب القناة أو الدولة التى تتبع لها وهم ليسوا إلا دمى تحركها السياسة المتعفنة , أما لو اخذنا أقنية الطرب والغناء فحدث ولاحرج كل يوم هناك مطرب أو مطربة جديدة وكل واحد يتسابق في أظهار نفسه بشكل أسرع وبالأخص مطرباتنا اللاشريفات التى يتسابقنا كل يوم في مسابقة من يخلع ملابسه أسرع يصل أسرع وكلها من اجل الفوز بالدنيا المادية التى نحن وهم يعلموا أن لافائز بها لكن هي حكمة الله فيهم , أما على صعيد الأفلام والمسلسلات فأبسط مثال للأنحطاط الأعلامي هو مناظر التقبيل والجنس اللامباشر الذي بدأت اراه وكأني أرى أعلان لعلكة سهام (أعلان سوري كان يعرض على التلفاز السوري ١٠٠٠٠٠ مرة يوميا) .

تصوروا أن كل هذه الأمور ألفناها ولم نعد نشعر بقذارتها وولم نعد نشعر بمدى تأثيرها على أمتنا وشبابنا وأجيالنا القادمة , فكون شعوب العالم الآخرى انحرفت فلقد كتب علينا أيضا الأنحراف , لكن لو فتحت عقلك الآن وبدأت تنظر إلى مايعرض في التلفاز على أنه شيئ قذر فسوف تكتشف كيف تم تغييبنا وكيف تم ابعادنا عن هدف الحياة الرئيسي .

يخرج علي متحدث ويقول لي أختر ماتريد أن تشاهده ولاتلتفت إلى هذه المحطات وهو يقصد فيها أقنية الدين والبرامج الأسلامية والتى أيضا وطئتها بعض العمليات المسيسة , وأنا أرد وأنا ميقن أن بعض القراء لن يعجبهم كلامي هذا وأعتبرها من الآن وجهة نظر تصيب أو تخيب , في الأعلام العربي هناك اكثر من ١٥٠ محطة دينية وبالأحصائيات وهناك أكثر من خمسين داعية سماعهم شيئ يسر له الخاطر وبرامجهم تعرض على التلفاز ٢٤ ساعة في اليوم فلو بدأت أتابعهم لوجدت نفسي من الصباح إلى المساء أتتبع كل واحد منهم ولا أنتهي ابدا , هناك من يتحدث عن الصلاة وهناك من يتحدث عن الزكاة وهناك من يخبرنا بسيرة رسول الله صلى الله عليه وسلم وكلها مواضيع قيمة جزا الله عنهم كل خير , لكن هل توقفت حياتنا على العبادات وتركنا العمل المفيد , هل أصبح الأسلام هو عبادات فقط ؟ , وهل نسينا حديث رسول الله صلى الله عليه وسلم في المرأة المتعبدة التى دخلت النار من أجل هرة , لن أخوض اكثر في هذا الموضوع فأنا أعلم أن المعنى وصل لكم .

الآن أقول أن قد صحوت من غفلتي والآن أشعر كيف كنت متعلقا بالتلفاز وبالأعلام القذر الذي أثر على كل جزء من حياتي سابقا فهو أما يجعلنا عاطفيين جدا أو يجعلنا قاسيين ولا وسط بينهما ولاعمل مفيد نقوله أمام الله بينهم , الآن أصبحت أتابع التلفاز لنصف ساعة فقط وهذه النصف ساعة هي عندما أذهب للنوم أو عندما أذهب للأكل فالتلفاز موجود في نفس الغرفة , أما أن أذهب مخصصا لكي أشاهد التلفاز فأنا والحمد لله لم أعد أذكر آخر مرة فكرت بهذا الامر , وخياري البديل هو الانترنت فكل ما ارغب بمشاهدته موجود هنا وفي اي ساعة وفي اي وقت أختار ما اريد أن أشاهده وأنتهى الأمر .

خلاصة كلامي هو أحذروا من الأعلام فوالله أن أصبحت أشبه أحيانا بالأعور الدجال الذي يقدم لك كل ماترغب به لكي تتوه في الدنيا وتنسى غاية الله في عباده , ومايعرض الآن سلبياته أكثر بكثير من إيجابياته وأقول لكم ما أقول وأنا شخص عاش وترعرع مدة طويلة في الغرب وشاهد على أعلامهم مايعقل ولا يعقل في وضح النهار وشاهدت بعض نتائج هذا الأعلام , أدعوكم من اليوم إما إلى التحقق من ماتشاهدونه من برامج وأفلام ومسلسلات وفيديو كليب من نظرة شخص مسلم أو أن تتوقفوا مباشرة عن متابعة أي شيئ ولتكن مشاهدتكم للتلفاز غير مقترنة بمتابعته ودمتم بود .

أيمن النعيمي - سوريا



Magazine

NetworkSet

First Arabic Magazine for Networks

مجلة NetworkSet مجلة الكترونية شهرية متخصصة تصدر عن موقع www.networkset.net

www.networkset.net

تقرؤون في هذا العدد

حقائق ومفاهيم خاطئة عن IPv6



بدايات الـ IPv6 كانت عام 1998، حيث كان المقصد الرئيسي من IPv6 هو حل مشكلة العدد المحدود من العناوين في IPv4، وعبر الزمن أضيفت العديد من الوظائف والميزات لهذا الإصدار , غير أن توسعة العدد المحدود من العناوين بقي هو الغاية من إيجاده. وخلال الأعوام الماضية تولدت العديد من المفاهيم الخاطئة والتي أثرت بنوع أو بآخر على فهم أمنية الشبكات التي تستعمل IPv6، لهذا فإنّ معرفة الحقيقة وراء هذه الأفكار الخاطئة يعتبر ضروري وخاصة الآن بعد ما أصبح هذا الايبي أكثر انتشاراً واستعمالاً يوما بعد يوم، لذلك سأبدأ في مقالي هذا بذكر أكثر الأخطاء المنتشرة اليوم.

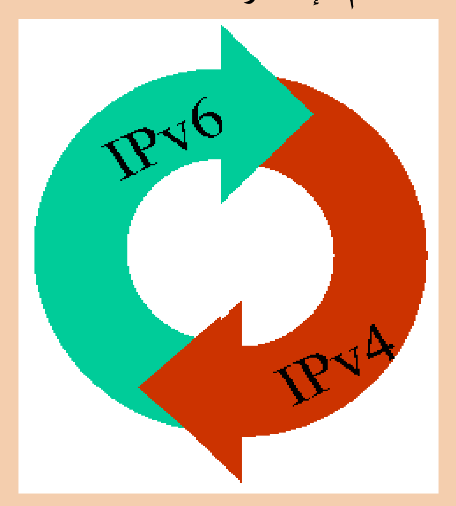


هل فعلا نحتاجه؟

أهم المفاهيم الخاطئة و أولها هو أننا لا نحتاج إلى IPv6، هذا الاعتقاد جاء نتيجة مرور أكثر من 12 عام منذ تطويره من دون الحاجة لاستخدامه بشكل كبير أو بمعنى آخر لم تستدعي الحاجة إليه، قد يكون صحيحاً ولكن في الوقت الحاضر فإنّ فكرة نفاذ IPv4 أصبحت واقعية ولم تعد بعيدة الوصول. حيث في بداية هذا العام 2011 وزعت منظمة IANA المسؤولة عن حجز العناوين آخر مجموعة من العناوين للموزعين المحليين RIRs ، وعلى الرغم من أن الأخيرة مازال لديها عدد من العناوين القليلة إلا أنها لن تبقى طويلاً إن لم تنتهي فعلاً , وذلك طبقاً لإحصائية تظهر معدل حجز يقدر بمليون عنوان IP جديد كل 4 ساعات.

نستطيع التحول عند الحاجة

البعض يعتقد إن التحول إلى IPv6 لن يحتاج إلى وقت طويل وسوف يتم تطبيقه بمجرد انتهاء عناوين IPv4 وهذا مفهوم خاطئ، فعملية التحول قد تحتاج إلى سنين قبل الانتقال كلياً إلى الإصدار السادس , حيث يستوجب هذا أن يكون كلا الإصدارين مستخدمين على الانترنت لفترة لكي يمكن التفاهم بين الأجهزة التي تستخدم الإصدارات المختلفة.



إلغاء الـ NAT سيقلل من أمنية الشبكة :

بما أنّ هناك عدد وافر من العناوين يقدمها IPv6 سينهي الحاجة إلى استخدام الـ NAT لذلك فالاعتقاد الآخر هو أنّ الشبكة سوف تكون أكثر عرضة للاختراقات وهذا خطأ أيضاً، فالكثير من المتخصصين يعتبرون أن عملية الـ NAT هي إحدى الخطوات

الأساسية لتأمين الشبكة، إلّا أنّ الحقيقة ليست في ذلك , فقد يكون اختراق الشبكة من داخلها ,فهي مجرد أداة وضعت لإعطاء الشبكة عنوان واحد يستخدم عبر الانترنت بدلاً من استخدام عدة عناوين لكل جهازٍ على الشبكة والذي ساعد على بقاء IPv4 صامداً طيلة هذه الفترة. فلماذا هذا التعقيد في الشبكة وإضافة حمل على أجهزتها بما أنّه لا يؤثر بشكل كبير على أمنية الشبكة على فرض تطبيق سياسات الحماية الأخرى.

جعل عملية النقل باستخدام QoS أفضل :

المفهوم الآخر هو إنّ الهيدر الخاص بـ IPv6 يحتوي على حقل من 20 بت يدعى Flow Label. وبهذا فإنّ هذا الحقل (الغير موجود في IPv4) يساعد على جعل عملية نقل البيانات عند استخدام QoS أكثر كفاءة، غير أنّ الحقيقة أنّه إلى الآن لم يستخدم هذا الحقل بشكل كبير, وأيضاً فهو لن يزيد شيئاً على سرعة النقل في الشبكات التي تستعمل QoS.



تقليل حجم Routing Table

كذلك من الأخطاء الأخرى هي أنّ IPv6 سيقلل من حجم الـ Routing Tables، وهذا مفهوم غير صحيح إطلاقاً , فعلى الرغم من إعادة كتابة بروتوكولات التوجيه لدعم IPv6 بشكل أفضل إلا أنّه لا يوجد تطوير حقيقي فعلي . حيث أنّ أبحاث الـ IETF منذ 15 عاماً ومازالت تحاول إيجاد حل لهذه المشكلة، ولكن بما أنّ عدد العناوين سوف يزداد فهو بحد ذاته ما يجعل الـ Routing Table مثله مثل IPv4 إذا لم يكن أكبر حجماً.

تقليل المشاكل الخاصة بـ BGP :

هذا المفهوم هو العكس بالضبط ، ليس فقط الـ Routing table لباقي البروتوكولات سوف يزداد، ولكن أيضاً الـ BGP table سوف يتطلب مساحة أكبر وكذلك باندويث أكثر من الذي يتطلبه IPv4 سابقاً.

IPv6 يعني شبكة أكثر أمناً :

من أكثر مفاهيم الأمن الخاطئة شيوعاً (كما ذكرنا في مفهوم الـ NAT) هو أن الشبكات التي تستعمل IPv6 هي أكثر أمناً من تلك التي تستعمل IPv4 بما أنّه سيدعم IPsec بشكل رسمي، فالعديد من الأشخاص ترجموا هذه العبارة بشكل خاطئ . أول شيء , إنّ IPsec سوف لن يحمي لوحده الشبكة من هجمات بروتوكول الـ IPv6، وحتى ولو حصل هذا فهو لا يمكن أن يُستخدم في جميع الاتصالات , فمثلاً بروتوكول الـ ICMP يستخدم الـ Multicast وبالتالي فإنّ استعمال IPsec لهذه الاتصالات الـ Multicast سيكون غير عملي وأيضاً لا يمكن استعماله في جميع الاتصالات عبر الانترنت. مختصر الكلام أنّ استخدام IPsec في شبكات IPv6 سوف لن يؤثر على أمنها , حاله حال IPv4 فالاثنين يستعملان سياسات الأمن المعروفة (ليس بالشكل نفسه للكل) ولكن لا يوجد بروتوكول أكثر أمناً من الآخر.

أخيراً أتمنى أن أكون قد غيرت شيئاً من المفاهيم الأكثر شيوعاً و المنتشرة على صفحات الانترنت , والتي يوجد الكثير منها لم أذكره، وإن شاء الله سوف أحاول تقديم تفاصيل أكثر في مقالات قادمة للتعرف على ذلك الضيف الجديد القديم في عالم الشبكات.

uRPF Security Feature



تعتبر خاصية uRPF أو unicast Reverse Path Forwarding من الخواص الأمنية المتاحة على الكثير من أجهزة cisco , فتعالوا نتعرف في هذا المقال على هذه الخاصية و أهميتها و كيفيه تطبيقها على Cisco Routers .

ما هي خاصية uRPF ؟

الهدف الرئيسي من تفعيل هذه الخاصية أو الهدف منها هو عملية التحقق Verifying لأي حزمة packet تصل إلى interface معين , أقصد هنا بعملية التحقق verifying هو معرفة مصدر الـ Packet و التأكد من صحتها و ليست عبارة عن Crafted OR Spoofed Packet .

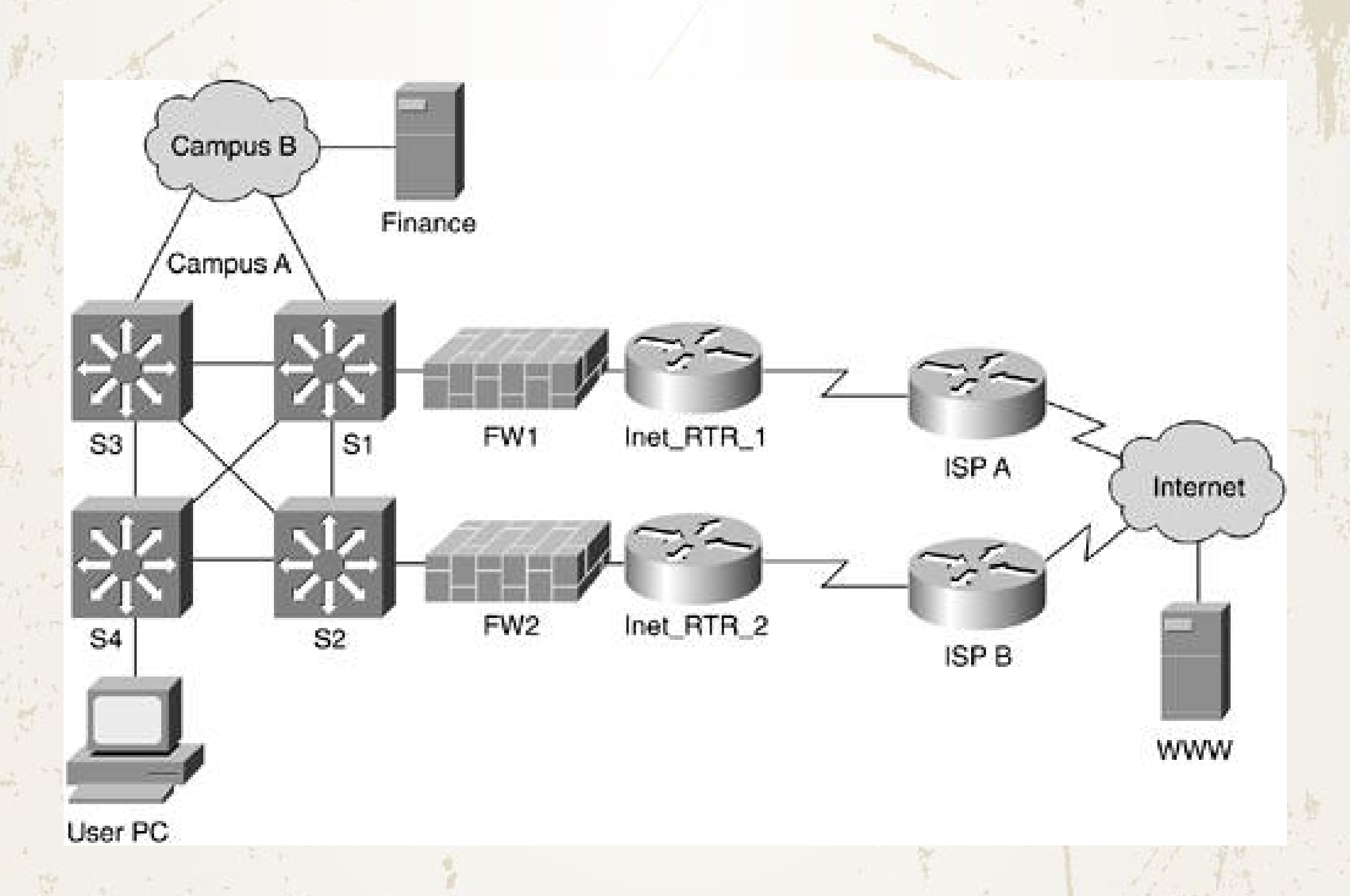
ولكن كيف يتم ذلك ؟ يتم ذلك عن طريق عملية تتبعها هذه الخاصية ما أي Packet تصل الى Interface مفعل به ال uRPF , فنعدما تصل ال Packet الى interface يتم عمل reverse path look-up اى يتم التاكد من المسار التى وصلت منه ال Packet ولكن بصوره عكسيه , تخيل معى ال Packet و هى تمر الى Interface مفعل عليه الخاصيه , اول شىء سيحدث هو التأكد من المسار بصورة عكسية كما قلنا و يحدث هذا عن طريق النظر الى شيئين هما ال Source IP for Incoming Packet و الشىء الثانى هو ال Routing Table , بعد ان عرفنا ال Source IP نقوم بالبحث عن مسار له بداخل ال Routing table فاذا وجدنا مسار ففى هذه الحالة يتم السماح لل Packet بالمرور بصورة عاديه جدا و ذلك لاننا نعرف طريق ال Source اذا فهو حقيقى و غير مزور Spoofed , اما فى حاله لم نجد اى Route لل Source IP ففى هذا الحالة يتم منع ال Packet من المرور و عمل Drop لها و السبب اننا لم نستطع التحقق من المصدر الذى هو حالتنا هذه ال Source IP . الخلاصة ان ال uRPF هى عبارة عن Security Mechanism لمنع عمليه ال IP Spoofing .

: uRPF Modes - Strict VS Loose

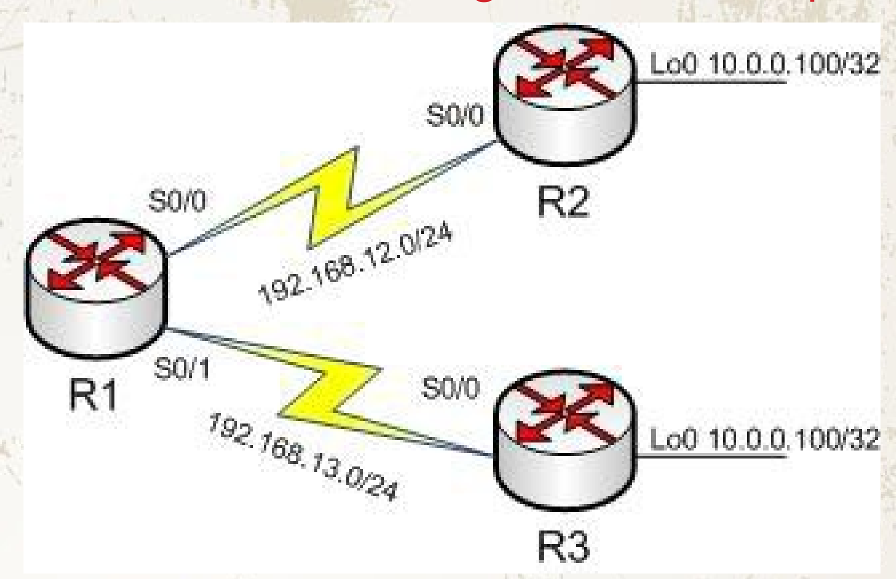
يوجد لدينا اكثر من Mode عند اعداد ال uRPF و هما :
(Strict Mode OR Loose Mode)

الـ Strict Mode هو مثل اسمه تماما الذى يعطى طابع الصرامة هو ايضا متشدد بشأن عمليه التأكد او ال Verifying فهو لا يكتفى فقط بالتاكد من وجود Route فى ال Routing Table لل Source IP لل Packet فقط , بل يشترط ان يكون هذا ال Route على نفس ال Interface الذى وصلت عليه ال Packet لنأخذ مثال للتوضيح , مثلا اذا وصلت packet على 0/f0 و قامت ال uRPF بالنظر الى ال Routing Table و البحث عن Route لل Source IP الموجود بال Packet ووجدت route و لكن عن طريق 1/f0 ففى هذه الحالة لا يتم السماح بمرور ال Packet , هذا هو ال Strict Mode اما بالنسبه لل Loose mode فهو بمجرد ان يجد Route لل source عن طريق اى interface يسمح فورا بمرور ال Packet عكس ال Strict Mode الذى يجب ان يجد مسار لل Source عن طريق ال Interface نفسه الذى وصلت ال Packet من خلاله .

فى حاله كان نستعمل ال Loose Mode و كان عندنا Default Route ففى هذه الحالة لا يعتبر هذا ال Default route صالحا لانه سيناسب اى Source IP هذا هو ال Default behavior و يمكننا تغيره عن طريق امر معين سنعرفه لاحقا اتمنى ان تكون هذه النقطة مفهومة .
نقطة اخيرة احب ان انبه عليها قبل ان نبدأ فى ال configuration و هى فى حاله قمنا بتفعيل ال strict mode و كان لدينا فى الشبكة اى سبب يمكن ان يودى الى ما يسمى Asymmetric Traffic flow سيسبب هذا بعض المشاكل و سيتم منع العديد من ال Traffic الامنه عن طريق الخطأ لان هذا الترافيك لا يأتى من ال Interface المتوقع ان يأتى منه . الصورة التالية تبين Toplogy قد يحدث بها Asymmetric Traffic flow اما اذا اردت معرفه المزيد حول ال Asymmetric Traffic flow يمكنك ان تبحث على الانترنت و ستجد العديد من المقالات تشرح هذا الامر .



: uRPF Configuration Example



المطلوب منا فى هذا المثال هو تفعيل ال uRPF على كل من S0/0 و S0/1 و ان يتم استخدام Strict Mode على R1.
ال configuration سيكون كالتالى :

```
R1# conf t
R1(config)# int S0/0
R1(config-if)# ip verify unicast source reachable-via?
  any Source is reachable via any interface
  rx   Source is reachable via interface on which packet was received

R1(config-if)# ip verify unicast source reachable-via rx?
  <1-199>           IP access list (standard or extended)
  <1300-2699>       IP expanded access list (standard or extended)
  allow-default     Allow default route to match when checking source address
  allow-self-ping   Allow router to ping itself (opens vulnerability in verification)

R1(config-if)# ip verify unicast source reachable-via rx
R1(config-if)# end
```

نبدأ بهذا الامر فى ال Interface كتالى R1(config-if)# ip verify unicast source reachable-via
و لكن يجب ان نختار اما ANY و هى تساوى Loose اما ان نختار rx و هى تساوى strict هذا فى اخر الامر السابق
طبعا , يوجد لدينا عدد من الخيارات بعد تحديد ال Mode منها Allow-default و هى تسمح لنا بالاعتماد على ال Default route فى عمليه التحقق من ال source , ايضا يوجد لدينا Allow-self-ping و تسمح للروتر ان يقوم بعمل Ping على نفسه لانه فى الحاله الطبيعيه لن يسمح ال uRPF بعمل ذلك .
هناك امر اخر سنحتاج اليه لكنه غير موضح بالصورة هذا الامر هو ip cef و نقوم بتطبيقة فى ال configuration mode و اهميه هذا الامر ان ال uRPF يعتمد احيانا على ال MIB .
اخيرا يمكن استخدام هذا الامر لنعرف اى mode تم تفعيله على interface معين

```
R1# sh run int S00/
!
interface serial00/
  ip address 80.1.1.1 255.255.255.0
  ip verify unicast source reachable-via rx allow-self-ping
```

بهذا نكون قد انتهينا من هذه الخاصيه و الى اللقاء فى موضوع اخر

Magazine

NetworkSet

First Arabic Magazine for Networks

معنى جديد لعالم الشبكات في سماء اللغة العربية









انقر على صورة المشروع
لزيارة صفحته على شبكة الانترنت



استخدم الأنابيب المناسبة في سباكة شبكتك

إنّ عملية توزيع الأسلاك في الشبكة يشبه كثيراً أعمال السباكة في المنزل, وكما تشكل الأنابيب الممرات التي تسمح بمرور المياه في سباكة المنزل فإن الأسلاك تشكل الممرات التي تسمح بمرور البيانات (إشارات كهربية داخل شبكتك. كمية البيانات التي تستطيع الحاسبات نقلها خلال الأسلاك تعتمد على خصائص هذه الأسلاك (الأنابيب) الموجودة, وكلما كبرت الأنابيب كلما زاد حجم البيانات التي يمكن للحاسبات أن تنقلها. ويمكننا أيضاً تشبيه حجم الأنابيب الموجودة في المنزل بما يعرف بالـ Bandwidth حيث يمثل الترددات القابلة للاستخدام ويقاس بالـ Hertz.

ويمكننا القول بأنّ الـ Bandwidth الأعلى يمثّل أنابيب أكبر لنقل البيانات. ولا يعني أنك تمتلك أنابيب كبيره أنه يتحتم عليك أن تملأهم عن آخرهم, لذلك فإنه من المنطقي أن تحاول قياس الحجم الفعلي للبيانات التي تسري خلال الأنابيب ويسمى بالـ Throughput, الأنواع المختلفة من الكابلات تؤدي إلى اختلاف معدلات تدفق البيانات في مختلف المسافات.

ويجب أن تتذكر أنه إذا كانت الأنبوبة كبيرة بما يكفي لتستوعب كل كمية المياه التي ترسلها إليها , إلا أنّه يمكن لهذا الأنبوب أنّ يصبح مسدوداً. كنتيجة, بالرغم من أنّه يمكن نظرياً لكمية محدده من البيانات أن تسري خلال كابل معين فإنّه في الحقيقة يمكن أن تجد معدلات تدفق للبيانات أقل من الـ Maximum Bandwidth الخاص بهذا النوع من الكابلات.

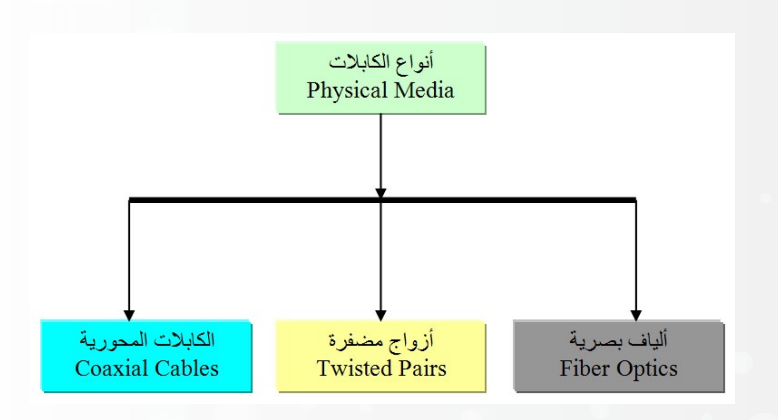
دائماً ما يقول السباكون أن الشوائب المعدنية والعوائق الأخرى دائماً ما تسبب إعاقة لسريان الماء في الأنابيب , أما الشّابكون (عاملو التشبيك) فيقولون أنّ هناك عوائق من شأنها خفض الأداء الفعلي للكابل الخاص بك , كالتداخل الكهرومغناطيسي مثلاً وهو ما يعرف بالـ (EMI).

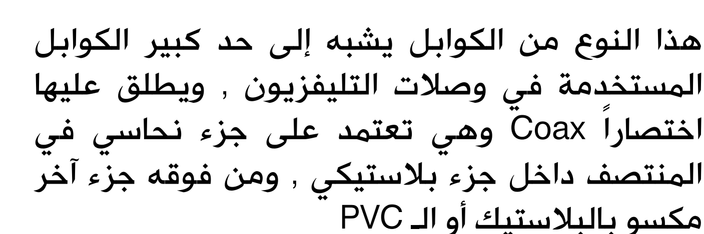
الطاقة الإنتاجية (Throughput) تقاس بـ Bits per Second(bps) فهي تصف الكمية الفعلية للبيانات التي تتدفق خلال الكابل في وقت معين. إذا أخذت أنبوباً وقمت بتقسيمه إلى أنابيب صغيرة فإنك للتو قد أعدت اختراع الـ Concept أو المفهوم الخاص بالـ Broadband Transmission (حيث يمكن نقل بيانات في ترددات مختلفة باستخدام نفس الوسط – الكبل مثلاً – بشكل آني), أما إذا بقى الأنبوب كاملاً بدلاً من تقسيمه فإنه يمثل الـ Concept أو المفهوم الخاص بالـ Baseband transmission (حيث يمكن استخدام الـ Bandwidth ليحمل مجموعة واحدة من الترددات لنقل البيانات مرة واحدة فقط في كل مرة).

فإن وُجدَ لدى السباكون أنواع مختلفة من الأنابيب كالبلاستيكية والمعدنية وغيرها فلدى الشابكون (عمال التشبيك) أيضاً أنواع مختلفة من الكابلات ونختصرها فيما يلي :

Physical media أو أنواع الكابلات

يشار إلى هذا المصطلح بالكوابل المستخدمة قي توصيل الشبكات وعلى الرغم من انتشار الشبكات اللاسلكية واستخدامها لتقنيات مختلفة في الاتصال بلا أسلاك أو كوابل إلا أن الشبكات السلكية تستخدم عدة أنواع من الكوابل سوف نتعرف عليها فيما يلي :





Coaxial Cables



هذا النوع من الكوابل يشبه إلى حد كبير الكوابل المستخدمة في وصلات التليفزيون , ويطلق عليها اختصاراً Coax وهي تعتمد على جزء نحاسي في المنتصف داخل جزء بلاستيكي , ومن فوقه جزء آخر مكسو بالبلاستيك أو الـ PVC

وهذه الكوابل لها نهايات طرفية خاصة لتوصيلها بكارت الشبكة والذي لابد أن يكون مجهزاً لتوصيل هذا النوع من الكوابل, والـ Connectors المستخدمة في توصيل هذه الكوابل تسمى BNC Connectors وهي Male و Female . إلاّ أنّ هذه الأنواع من الكوابل يحدث بها ما يسمى Signal bounce أو ارتداد الإشارة مرة أخرى من نهاية الكابل إلى داخله, ولهذا فإنها تحتاج إلى Terminators في النهاية لامتصاص الإشارات حتى لا تنعكس مرة أخرى في الكابل وتؤدي إلى مشاكل كبيرة في الشبكة وفقد للبيانات.







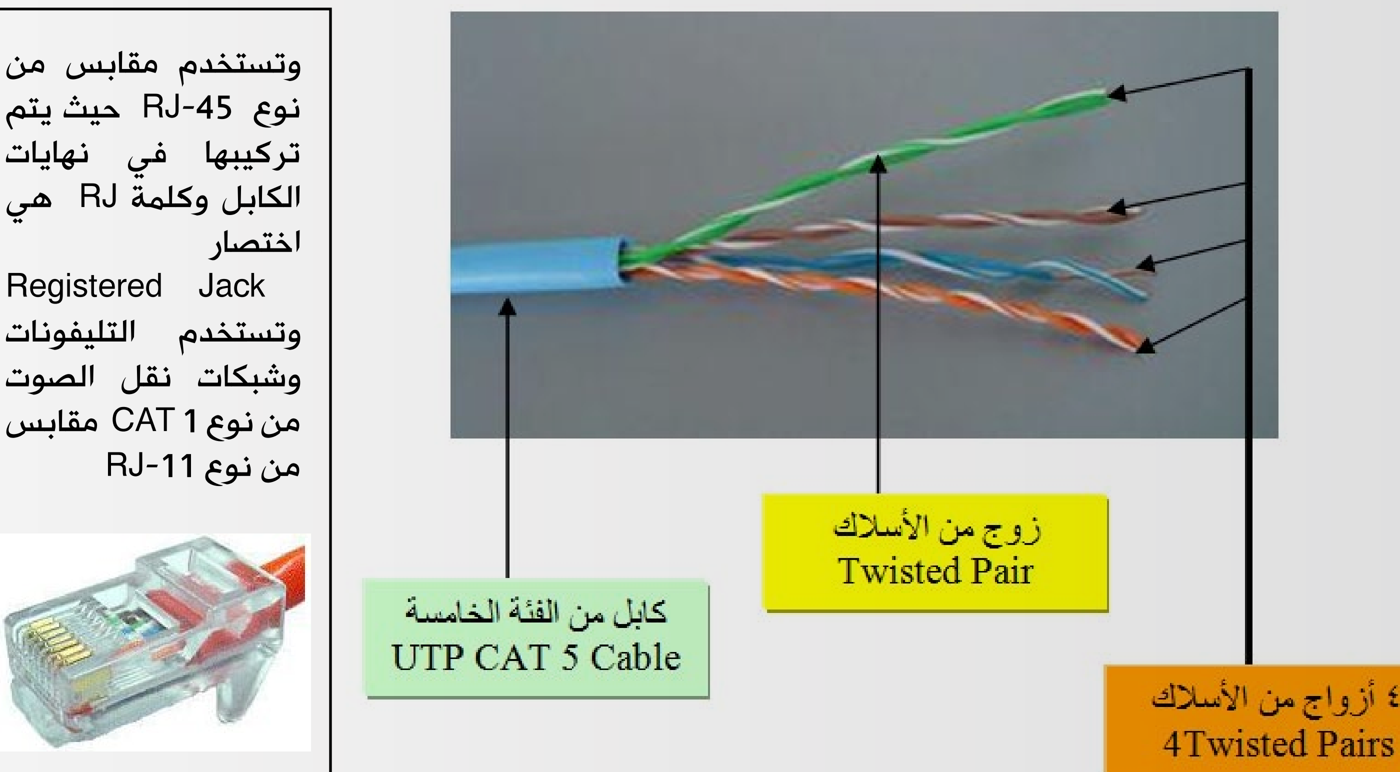
Twisted Pair Cables

هذا النوع من الكوابل هو الأكثر شيوعاً هذه الأيام , وهو عبارة عن مجموعة من الأزواج من الأسلاك Pairs يتكون منها الكابل الأساسي, وتنقسم إلى قسمين UTP أو Unshielded Twisted Pairs وهي الكوابل الغير معزولة وهي, مستخدمة أكثر في شبكات Star وهناك النوع الثاني وهو STP أو Shielded twisted pairs

ويستخدم أكثر في شبكات Token Ring والكوابل لها فئات وأنواع مختلفة تعرف باسم CAT اختصاراً لـ Category وسوف نتعرف عليها فيما يلي :



CAT 1	يتكون من 4 أسلاك أو زوجين وهو غير مناسب لنقل الـ DATA وغالبا ما يستخدم في التليفونات
CAT 2	8 أسلاك أو أربع أزواج من الأسلاك 4 Twisted Pairوهو صالح لنقل 4Mbps
CAT 3	8 أسلاك أو أربع أزواج من الأسلاك 4 Twisted Pairوهو صالح لنقل 10Mbps
CAT 4	8 أسلاك أو أربع أزواج من الأسلاك 4 Twisted Pairوهو صالح لنقل 16Mbps
CAT 5	8 أسلاك أو أربع أزواج من الأسلاك 4 Twisted Pairوهو صالح لنقل 100Mbps
CAT 6	8 أسلاك أو أربع أزواج من الأسلاك 4 Twisted Pairوهو صالح لنقل 1000Mbps





وتستخدم مقابس من نوع RJ-45 حيث يتم تركيبها في نهايات الكابل وكلمة RJ هي اختصار Registered Jack وتستخدم التليفونات وشبكات نقل الصوت من نوع CAT 1 مقابس من نوع RJ-11

Ethernet Cable Description

سوف نتطرق في هذا الجزء إلى وصف أنواع الكوابل المستخدمة في تشبيك شبكات Ethernet لأنه سيقابلك في أي تعامل مع الشبكات. هل رأيت هذا الكود على أحد الكوابل أو في أي كتاب يهتم بالشبكات 100BaseT ؟

بالتأكيد رأيته ولكن ماذا يعني ؟

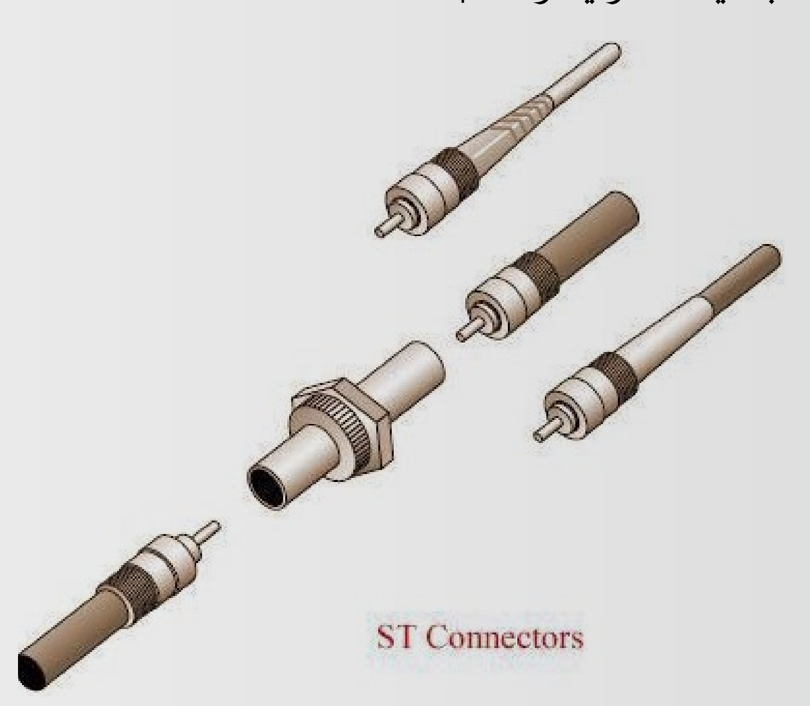
هذا هو ما يسمى الوصف الكودي للكوابل المستخدمة ويعبر عنها بمعادلة بسيطة تدعى N<Signal>X

وتعني عموماً ما يلي N هو سرعة الكابل أي 100 Mega bit/Second على سبيل المثال , أما Signal فهو يعبر عن نوع الإشارة المستخدمة داخل الكابل, هل هي Base والتي تعني Baseband أو Broad والتي تعني Broadband , أما الـ X غالباً تعني مواصفة معينة للكابل تختلف ما بين الكوابل وهي خاضعة للمعهد الأمريكي للهندسة IEEE , فمثلاً عند رؤيتك حرفي الـ T أو الـ F في أي وقت عليك بتبديل الحرف T بـ Twisted-Pair والحرف F بـ Fiber-Optic , فعلى سبيل المثال10baseT تعني أن هذا الكابل يعتمد على الـ baseband يدعم سرعة تصل إلى 10MBps مستخدماً الـ Twisted-Pairs, وعلى نفس النمط 10baseF تعني نفس الشيء فيما عدا أنّها تستخدم كابلات الـ Fiber-optics بدلاً من الـ Twisted-pairs.

Fiber-Optic Cables

هذا النوع من الكوابل باهظ الثمن وتستخدم هذه الكوابل تقنية نقل البيانات باستخدام الضوء ولهذا جاء المسمى بالألياف الضوئية أو Fiber Optics .

وتستخدم هذه الكوابل مقابس توصيل أشهرها ST Connectors أو Straight Tip Connectors و SC Connectors أو, Subscriber Connectors ويجب أن تضع في الحسبان أن هذا النوع من الكوابل يستخدم لنقل البيانات عبر عدة كيلومترات وليس عدة أمتار كما في كوابل CAT 5 ومثيلاتها, فهو يعتمد على سريان الضوء في الكابل وانعكاسه لمسافات طويلة تعتمد على نوع الكابل قد تصل إلى 4 كيلومترات أو أكثر , إلّا أنّه كما ذكرنا فهو صعب التركيب وباهظ التكاليف , ويستخدم عادةً في عمل الـ Backbone و التوصيل ما بين المباني والأماكن البعيدة عن بعضها البعض , والتي لن تستطيع توصيلها بـ UTP cables أو حتى بالـ Coaxial .



ST Connectors



SC Connectors



وفي النهاية نقول كما أن السباكة الجيدة مهمة جداً في بناء بيت بدون تسريبات أو انسدادات في الأنابيب الموجودة به , فإنّ الشبكة الجيدة تتطلب منك معرفة بأنواع الكابلات وخصائصها لكي تتمكن من بناء شبكة جيدة خالية من التداخلات والانقطاعات المتكررة.


لمحة عن الكاتب
أيمن النعيمي
الجنسية : سورية
مهندس شبكات سوري
مؤسس أول مجلة وموسوعة عربية في الشبكات
حائز على عدة شهادات علمية ومهتم بالمحتوى العربي على الأنترنت
admin@networkset.net

رابع
خطوات إحتراف عملية الـ Backup

لقد وصلنا اليوم إلى جزئنا الرابع وما قبل الأخير في خطوات احتراف عملية النسخ الاحتياطي , والتي سوف أخصصها للحديث عن كيفية اختيار وسائط التخزين المناسبة لحفظ البيانات , وما هي أهم النقاط الواجب مراعاتها في عملية الأختيار. ويفضّل قبل متابعتك لقراءة التدوينة مراجعة الأقسام السابقة : الاول , الثاني , الثالث .

قد يكون حديثنا في هذا الموضوع ليس بالشيء الهام جداً , لأننا سوف نتناول بعض وسائط التخزين التي قد لا تستخدم في حياتنا الواقعية والعملية , لكن حرصاً منّي على نشر الخطوات الأكاديمية لعملية إدارة وأحتراف النسخ الأحتياطي أطرح هذا الموضوع .
قبل أن ندخل في وسائط التخزين المتاحة , يتوجب علينا أولاً أن نجيب على بعض النقاط الهامة قبل أن نقرر ماهو الوسيط المناسب للملفات التي لدينا , لأنَّ أجابتنا على هذه الأسئلة هي من ستقوم بتحديد أفضل وأنسب خيار لدينا , وخصوصاً أن عملية اختيار الوسيط المناسب تعتبر من أهم الأجزاء في عملية النسخ الاحتياطي , والأسئلة سوف تكون على الشكل الآتي :
ما هو نوع الملفات وما حجمها ؟ وقد ناقشنا هذا السؤال في تدوينات سابقة .
ما هي مقدار الثقة التي تحتاجها من وسيط التخزين ؟ والمقصود بهذا السؤال , هل ترغب بوسائط قوية وأمنة لاتتأثر بالهزات الأرضية أو الحرائق أو الصدمات ؟.

ماعددة مرات النسخ الاحتياطي التي تقوم بها ؟ والمقصود بهذاالسؤال , هل تقوم بعمل نسخ احتياطي بشكل متكرر و يومي أو أسبوعي أو شهري ؟.
سهولة نقلها وحملها ؟ والمقصود بهذا السؤال , هل ترغب أن تكون الوسائط من النوع الذي يمكن نقله بسهولة أم أنّ موضوع النقل غير مهم و أنّها ستبقى هذه الوسائط في مكان واحد ؟.
هل أعتمد على برنامج معين في النسخ ؟ أحياناً نقوم بعملية النسخ الاحتياطي اعتماداً على برامج وتطبيقات معينة , لذلك يتوجب علينا مراعاة الوسائط التي يدعمها البرنامج , فعلى سبيل المثال : هل يدعم البرنامج عمل نسخ احتياطي على سيديات عادية ؟ .
والسؤال الأخير , ما هي الميزانية المتاحة لديك ؟
كل أجوبة هذه الأسئلة تعد جزء من عملية اختيار أفضل وسيط في عملية التخزين , وكما اتفقنا في بداية المقال أنّ الموضوع الآن أصبح لا يحتمل خيارات كثيرة في عملية الاختيار بسبب ظهور وسائط تخزين كبيرة ورخيصة في نفس الوقت , اما من الناحية الأكاديمية فالاختيار يعتبر صعباً بعض الشيء , ولا يمكن تحديد الوسيط الأفضل لأنّ لكل منهم إيجابيات وسلبيات مرتبطة بالأسئلة السابقة.

Backup to Floppy Disk (FD)

الوسيط الأول : أعتقد أن بعضكم يجدر به أن لا يعرف ما هو , فحجمه البالغ 1,4 ميغا فقط جعله أسوء وسيط تخزين في العالم , لكن في السابق كان الأفضل واليوم هو الأسوء , من ميزاته يمكنك الكتابة والازالة متى أردت , سلبياته هي أنّ حجمه صغير جداً وسرعته بطيئة.



Backup to Hard Disk Drive (HDD)

الهارد ديسك بشقيه الداخلي والخارجي : هو الرقم واحد في العالم الآن , والذي جعله على قائمة التصنيف هو



مراعاته لكل المتطلبات في آن واحد , ومن مزاياه سرعة كبيرة في عملية النسخ والأسترجاع للنسخ الاحتياطية , و المساحات الكبيرة , أما سلبياته فهي تتمثل في حمايته لأنّنا نعلم أن الهارد لو سُرق أو تعطل فالمشكلة يمكن أن تكون غير محدودة بالنسبة للشركة و أمنها بالإضافة إلى صعوبة حملها .

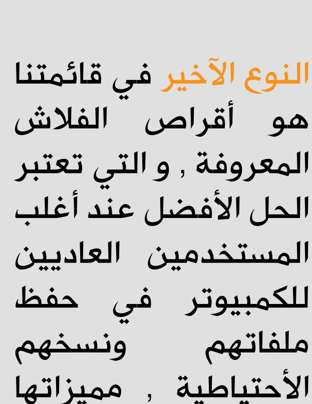
Backup to optical disks

الأقراص البصرية : يمكن تصنيفها أيضاً ضمن الوسائط المتاحة في عملية النسخ الاحتياطي , ما يميزها هو سعرها الرخيص , سرعة جيدة (أقل بمرتان أو ثلاثة من الهاردات) , سهولة في الحمل , أحجامها تبدأ من 128 ميغا وتصل إلى 6 غيغا كحجم أقصى , أما سلبيات إستخدام هذه الأقراص فهي تتمثل في درجة الوثوقية للملفات المخزنة . أما أنواع هذه الأقراص فهي على النحو الآتي :

CD-ROM (compact disk - read only memory)
CD-WORM (write once read many)
CD - RW (rewritable compact disk)
DVD(digital versatile disk or digital video disk)

أقراص الدي في دي : تعتبر أيضا نوعاً من أنواع الأقراص البصرية الصالحة لعملية النسخ الاحتياطي , لكنها تعمل بتقنية مختلفة بعض الشيء عن الـ Compact Disk , من مميزاتها تتمثل في أحجامها الكبيرة فهي, تبدأ من 4,7 غيغا وتصل إلى 17 غيغا , سرعة جيدة وأفضل من الأقراص العادية, تبدأ من 600 كيلو وتصل إلى 1,3ميغا في الثانية . أما أنواع هذه الأقراص فهي نوعان :

DVD - R (DVD-Recordable)
DVD - RW (DVD-ReWritable)
Backup to Compact Flash (CF)



النوع الآخير في قائمتنا هو أقراص الفلاش المعروفة , و التي تعتبر الحل الأفضل عند أغلب المستخدمين العاديين للكمبيوتر في حفظ ملفاتهم ونسخهم الأحتياطية , مميزاتها كثيرة مثل أحجام كبيرة تبدأ من 1 غيغا ولايوجد لها نهاية محددة لأنّ هناك عمل متواصل في زيادة حجمها , سرعة تعتبر جيدة وأفضل من الأقراص العادية , سهولة كبيرة في النقل , أمان أكبر من السيديات .



إلى هنا نكون قد أنتهينا من القسم الرابع من خطوات أحتراف عملية النسخ الاحتياطي , والتي كانت مخصصة للحديث عن وسائط التخزين , وكلمتي الأخيرة حول وسائط التخزين هي بخصوص الثقة , لاتثق بأي وسيط تخزين مهما كانت شهرته وقوته , فهي في النهاية ألآت مبرمجة لتعمل وفق طريقة معيّنة , لذلك لا تثق بها , وأعمل دائماً على توفير أكثر من وسيط لتخزين الملفات , أتمنى أن تكونوا قد حصلتم على معلومة ولو صغيرة أفادتكم , ولنا موعد أخير إن شاء اللّه لنتكلم عن البرامج والأدوات المستخدمة في عمل النسخ الاحتياطي , ولا تنسونا من دعواتكم ودمتم بود



تتقدم إدارة موقع

NetworkSet

First Arabic Magazine for Networks

بالشكر والتقدير للمهندس السوري

عثمان اسماعيل

تقديرا لمبادرته الطيبة في مراجعة المقالات والتدقيق الإملائي في المجلة

مؤسس ومدير موقع NetworkSet

المهندس أيمن النعيمي

2011 / 10 / 28





ألاحظ العديد من الطلاب يهملون قراءة الكتاب في مرحلة الإعداد لإحدى الشهادات التقنية، ويكتفون بمشاهدة الفيديوهات التعليمية و أعتبرها خطة فاشلة للدراسة وأنصح جميع الإخوة بالتركيز على الكتاب لما فيه من شرح كافي و معلومات قيمة وذلك لبناء أساس صلب و قوي لن يتهاوى عند أول مقابلة للحصول على الوظيفة. وحينها ستعرف أن الشهادة هي بمثابة جواز لك للحصول على المقابلة ويجب عليك أن تكون فاهم فهما دقيقا للمعلومات المتواجدة في الشهادة لإقناع المشغل بمؤهلاتك، وإلا ستندم يوم لا ينفع الندم ، لهذا خصصت هذا الموضوع حول أحد الكتب الرسمية لشهادة الCCNP .

اسم الكتاب :	Official Certification Guide 902-CCNP ROUTE 642
اللغة : الانجليزية	اسم المؤلف: Wendell Odom
دار النشر: Cisco Press	سنه الاصدار: 9 فبراير2010
	عدد الصفحات : 768

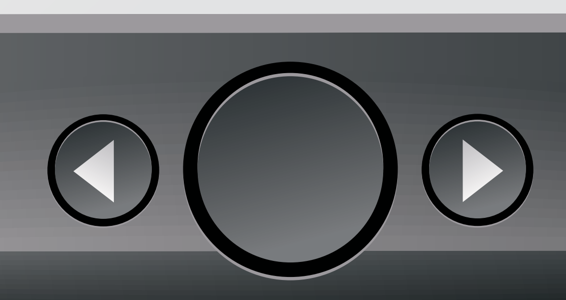
نبذة عن الكتاب :

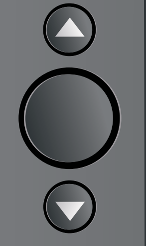
كتاب ال 902-CCNP ROUTE 642 Official Certification Guide هو إحدى الكتب الأساسية لمنهاج شهادة الCCNP . وفقراته تركز تحديدا على أهداف إمتحان الCCNP ROUTE . في هذا الكتاب يقوم السيد ويندل أودوم وللإشارة فهذا الكاتب يعتبر في لائحة كتاب الBest-Selling ، بتقديم العديد من التلميحات والنصائح لتسهيل عملية اجتيازالإمتحان. وهو يساعدك في تحديد مناطق الضعف الخاصة بك و تحسين الجانب النظري ومهارات التدريب العملي على حد سواء. هذا الكتاب يمكن دراسته أيضا للتعلم فهو يفسرالعديد من المفاهيم المتقدمة حول الشبكات ، ويبين كيفية تحويل هذه المفاهيم إلى عمل تطبيقي على أجهزة سيسكو، ويشرح كيفية تحديد إذا ما كانت هذه الإعدادات تعمل جيدا. إذ يمكنك استخدام هذا الكتاب كمرجع عام لبروتوكولات الIP Routing

.ومع ذلك ، يبقى الدافع الأساسي لكتابة لهذا الكتاب هو مساعدتك على اجتياز الامتحان .

من ميزات هذا الكتاب أنه يعطيك العديد من الأدوات التي تساعدك على تحديد ومراجعة ما تعرفه، وتعلم ما لا تعرفه، وسوف يجعلك مستعدا للامتحان إن شاء اللّه. هذه الميزات تشمل :

- Do I Know This Already?"" Quizzes : كل فصل يبدأ باختبار يساعدك على تحديد الوقت اللازم الذي تحتاجه لدراسته.
- Foundation Topics : هذه هي الأجزاء الأساسية من كل فصل. فهي تشرح البروتوكولات، المفاهيم والإعدادات.
- Exam Preparation Tasks : تسرد سلسلة من الأنشطة الدراسية التي ينبغي القيام بها بعد قراءة ال Foundation Topics section. كل فصل يتضمن أنشطة تجعلك تعرف مدى استيعابك لمواضيع هذا





كتاب أعجبني

الفصل.
CD-based practice exam : يحتوي القرص المضغوط محاكيا للامتحان يضم 100 سؤال متعدد الخيارات.

- Companion website : موقع http://www.ciscopress.com/title/9781587202537 يضم بعض توضيحات المواضيع المعقدة. أدخل على هذا الموقع بانتظام لأنك ستجد منشورات جديدة وحديثة كتبها المؤلف.

مواضيع هذا الكتاب منظمة في سبعة أجزاء رئيسية. الجزء 1 و7 يشملان مواضيع غير متعمقة من الناحية التقنية، بعكس الأجزاء من 2 إلى 6.

عنوان جزء الأول هو Perspectives on Network Planning: يتكون من فقرة واحدة تتحدث عن تصميم الشبكة(network design)، خطط التنفيذ(implementation plans) وخطط التحقق(verification plans)

يبدأ الجزء الثاني وهو تحت عنوان EIGRP مكون من ثلاث فقرات باستعراض أساسيات الEIGRP ويقوم بتذكيرك بكل مادرسته في مستوى الCCNA . بعد ذلك يقوم الكاتب بشرح العديد من المفاهيم المتقدمة حول ال EIGRP ككيفية تكون Routing, Nighbors & Topology table و ال Convergence. ثم يقوم بإعداد EIGRP authentication ، route summarization. و route filtering.

الجزء الثالث أتى تحت عنوان OSPF و هو مكون من أربع فقرات يبدأ بالتذكير بأساسيات الOSPF ، بعد ذلك ينتقل الكاتب لشرح عدة مواضيع متقدمة حول ال OSPF ككيفية تكون Routing, Nighbors & Topology table و ال Convergence.

ثم يقوم بإعداد OSPF authentication ، route summarization، route filtering و . Default Routingفي الفقرة الأخيرة يتكلم الكاتب حول ال OSPF virtual links و استعمال الOSPF في شبكات non-broadcast multiple access network (NBMA) كالFrame relay .

الجزء الرابع مكون من 3 فقرات تحت عنوان الPath Control ، يتحدث حول أدق تفاصيل الIGP Redistribution ، ال Policy Routing و ال IP Service Level Agreement .

عنوان جزء الخامسBGP وهولا يحتاج إلى أي معرفة مسبقة بالBGP ، مكون من 3 فقرات، تتطرق إلى أساسيات ال BGP و مقارنة بينه وبين الIGPs ، جدوى استعمال الBGP configuration ، BGP verification – و الInternal BGP and BGP Route Filtering .

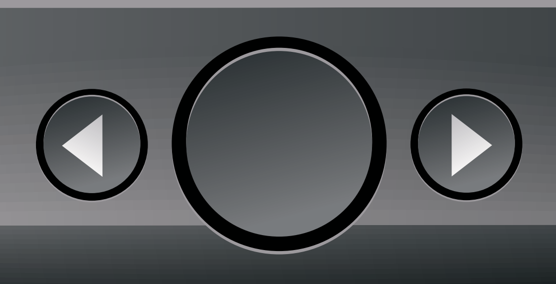
يتحدث الجزء قبل الأخير عن الIPv6 Addressing ، ال IPv6 Routing Protocols-Redistribution و ال IPv4 and IPv6 Coexistence .

الجزء الأخير Routing over Branch Internet Connections يتكلم عن ال IPsec/GRE tunnels، ال DHCP server, ، الNAT و الDSL .

يختتم الكتاب بفقرة تقترح استراتيجيات للإعداد النهائي قبل ولوج الامتحان.

صراحة أعتبرهذا الكتاب من أفضل الكتب التي قرأتها حول الشبكات، إذ يقوم الكاتب باستعمال أسلوب بسيط وسلس أثناء الشرح ، وهو غزير بالمعلومات القيمة و المفصلة حول الشبكات و أنصحكم يا إخواني بقراءته وأعدكم أنكم سوف ستستمعون بإذن الله خلال رحلتكم مع ويندل أودوم .







الذاكرة المنخفضة في راوترات سيسكو.
أسباب وحلول!!



لمحة عن الكاتب
فادي أحمد الطه
الجنسية : العراق
مهندس كمبيوتر ومعلوماتية واحضر حاليا لاكمال الدراسات العليا في تخصص شبكات الكمبيوتر. هدفي المساهمة في تطوير العالم
f_altaha88@yahoo.com

مشاكل الذاكرة الموجودة في الراوتر لم تعد جديدة , وعلى الرغم من أنّها لم تعد كثيرة كما كانت ولكن مازالت تظهر من حين لآخر. هذه المشكلة والتي تزعج المستخدمين عادة تختلف حسب الضرر الذي تحدثه وتتنوع أضرارها من انهيار النظام إلى توقف الراوتر عن عمل الـ routing، أما إذا كنا محظوظين فكل ما يحدث هو إن الراوتر سيبدأ بفقدان الـ routes ويتصرف بشكل عشوائي وغير مستقر وهذا الأمر أيضا غير مقبول على الإطلاق.

بعد أن تعرفنا على المشكلة وأضرارها نأتي الآن إلى أسبابها والتي قد تكون:

- عطل هاردوير في الذاكرة.
- أخطاء برمجية.
- استنزاف الذاكرة من قبل بعض الـ services أو البرامج.
- الإعدادات الخاطئة.

ولكن من أهم العوامل التي تؤدي إلى استنزاف الذاكرة هو بروتوكول الـ BGP فهو يقوم بمعالجة كميات كبيرة من الـ routes مقارنة مع بروتوكولات الـ routing الأخرى , لذلك فهو يعتبر من أكثر البروتوكولات استهلاكا للذاكرة. حيث أصبح ذلك شائعا خصوصا عند عبور الـ count limit الخاص بالـ route.

حالات الذاكرة وخطورتها :

تتغير حالات استهلاك الذاكرة حسب خطورتها، لكن بشكل افتراضي يتعامل بروتوكول الـ BGP (والذي سنأخذه كمثال للتطبيق) مع حالات الذاكرة المنخفضة كالتالي (مع العلم إنها غير ثابتة ويمكن تغيير قيمها) :



(Minor alert (85%: تعتبر هذه الحالة أقل الحالات خطورة , حيث يتوقف بروتوكول الـ BGP عن بدء أي route جديدة ولكن لحسن الحظ ستبقى الـ routes القديمة موجودة.

(Severe alert (90%: هذه الحالة هي الثانية في درجة خطورتها حيث يقوم بروتوكول الـ BGP بإيقاف routes معينة كل دقيقتين حتى تتحول الحالة إلى minor. والتي تعتبر بالفعل حل جيد بدلاً من فقدان جميع الـ routes. ولكن كيف يختار البروتوكول الـ route التي يجب إيقافها ؟

الطريقة كالتالي: يقوم البروتوكول بحساب النسبة بين مجموع الـ paths التي تم استلامها و مجموع الـ paths التي حددت كأفضل path لكل راوتر. مثال: إذا فرضنا أن الـ paths التي استلمناها مجموعها 60 ومجموع الـ paths التي حددت كأفضل path هو 40 , إذن ستكون النسبة 3:2, لذلك فالـroute ذات الأعلى نسبة سوف يتم إيقافها وهذا شيء منطقي لكونها الأقل أهمية.

الشيء الرائع أيضاً في هذه الحالة هو أنّنا نستطيع تحديد الـ route التي يختارها الراوتر لكي يتم إيقافها بقصد المحافظة على route أكثر أهمية حسب اعتقادنا و كما سنرى بعد قليل.

(Critical alert (95%: الحالة الاستثنائية والأكثر خطورة ,لذلك يقوم الـ BGP بإيقاف جميع الـ routes بشكل نهائي وبصورة تدريجية.

بعد أن تعرفنا على هذه الحالات نأتي الآن لنلقي نظرة على رسائل الـ log التي تظهر في cli الراوتر عند حدوثها وهي كما وضحت سابقاً :

```
%PLATFORM-2-MEMORY_ALERT: Memory Status Alert : MINOR
%PLATFORM-2-MEMORY_ALERT: Memory Status Alert : SEVERE
%PLATFORM-2-MEMORY_ALERT: Memory Status Alert : CRITICAL
```

وحين استعادة جزء من الذاكرة تتغير رسائل الـ log إلى:

```
%PLATFORM-2-MEMORY_ALERT: Memory Status Alert : MINOR ALERT RECOVERED
%PLATFORM-2-MEMORY_ALERT: Memory Status Alert : SEVERE ALERT RECOVERED
%PLATFORM-2-MEMORY_ALERT: Memory Status Alert : CRITICAL ALERT RECOVERED
```

أما عندما تتوقف إحدى الـ route كما رأينا في Severe alert تظهر هذه الرسالة :

```
%BGP-2-PEERSHALTED:  bgp-100 [5440] ; BGP 10.1.5.99 shutdown due to no memory
condition (Severe Alert)
```

كيف نعرف حالة الذاكرة الآن؟

```
Router# show system internal memory-status
MemStatus: Severe Alert
```

لاستعراض حالة الذاكرة حاليا نستعمل الأمر show والتي يظهر فيها أن الذاكرة وصلت إلى حالة الـ Severe Alert :
كما يمكننا وبشكل آخر استعراض حالة الراوتر من حيث عدد الـ process التي يعالجها حاليا وحالة الـ CPU و الذاكرة وغيرها وبالتأكيد عن طريق الأمر Show:

```
Router# show system resources
Load average:   1 minute: 0.23   5 minutes: 0.22   15 minutes: 0.20
Processes    :   980 total, 1 running
CPU states   :   3.0% user,   2.5% kernel,   94.5% idle
Memory usage:   4115812K total,   2885968K used,   1229844K free

Router# show routing memory estimate
Shared memory estimates:
  Current max     32 MB;  27495 routes with 16 nhs
          in-use   1 MB;     67 routes with  1 nhs (average)
  Configured max  32 MB;  27495 routes with 16 nhs
```

تغيير إعدادات الذاكرة:

الآن وصلنا إلى أهم جزء في هذا المقال وهو تغيير إعدادات الذاكرة وكيف نستثني route من الإيقاف من قبل الراوتر، والطريقة كالتالي :
بدايةً نقوم بتفعيل الـ BGP في الراوتر:

```
Router(config-router)# router bgp [AS NUMBER]
```

لإعداد الراوتر المطلوب استبعاده:

```
Router(config-router)# neighbor [peer address] remote-as [AS NUMBER]
```

تفعيل خيار الاستثناء لهذا الـ rout

```
Router(config-router-neighbor)#low-memory exempt
```

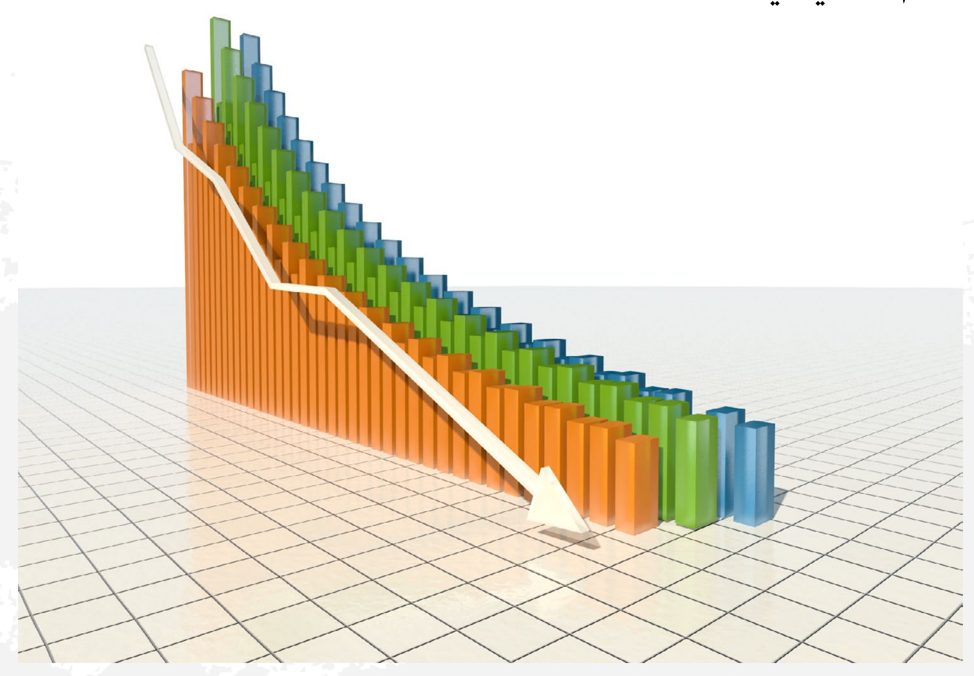
ومثل ما وضحنا أنّه يمكن تغيير قيمة النسبة التي تتغير عندها الحالة وهي كالتالي:

```
Router (config)#system memory-thresholds minor {%} severe {%} critical {%}
```

ولمنع الراوتر من إيقاف الـ routes عند الوصول إلى حالة الـcritical نستعمل الأمر التالي (على الرغم من أنّ سيسكو لا تنصح بهذه العملية) :

```
Router (config)#system memory-thresholds threshold critical no-process-kill
```

أخيرا وكما ذكرت فإنّ حالة الذاكرة المنخفضة لم تعد منتشرة في الشبكات البسيطة نظرا لوجود راوترات ذات مواصفات كافية , ولكن قد تحدث غالبا في راوترات الانترنت ومجهزي الخدمة الرئيسيين ISP.
إلى هنا ينتهي مقالنا اليوم ونلتقي في مقال آخر بإذن اللّه.



تعرّف على شركة HUAWEI


لمحة عن الكاتب
محمد جمال ثابت
الجنسية : مصر
طالب بكلية تجارة- 20 سنة
ولكن محب لدراسة الشبكات
وأطمح في الحصول على ثلاثة
.ccie
mohamedgamal_it@hotmail.com



1) تعتبر هواوي من الشركات العالمية المتعددة الجنسيات في مجال الاتصالات والشبكات , تأسست عام 1988 في مدينة Shenzhen الصينية والتي تقع شمال مدينة Hong Kong.



2) هي شركة خاصة مملوكة من قبل موظفيها وتأسست على يد (Ren Zhengfei) , وهو الرئيس والعضو المنتدب لشركة هواوي , وكما ذكر في مجلة Forbes الأمريكية أن رئيس شركة هواوي من اغني الأشخاص الموجودين في الصين والتي بلغت الأصول الشخصية التي يمتلكها حوالي 124 مليون دولار أمريكي (ربنا يعطينا ويعطيكم). كما أنه من اقوي 7 رجال أعمال في قارة أسيا.


PHOTO: IMAGINECHINA



3) هي أكبر شركة في الصين تقدم موارد ومعدات تهتم بمجال الشبكات والاتصالات السلكية واللاسلكية , وهي ثاني أكبر مورد في العالم , يقوم بتقديم معدات وبنية تحتية خاصة بالـ(mobile telecommunication) وذلك بعد شركة أريسكون التي تحتل المركز الأول في هذا المجال.

وبدأت هواوي برأس مال RMB 21,000 وهي العملة الرسمية للشعب الصيني وهي اختصار لـ (Renminbi).وأخذت هواوي أول توكيل مبيعات لها من شركة بهونج كونج منتجة لسويتشات تسمى (PBX) Private Branch Exchange.

تاريخ الشركة

للتعرف علي تاريخ الشركة وتقدمها يجب أن نعلم ما هو السبب الرئيسي وراء هذا التقدم؟ في الحقيقية سبب وتطور هذه الشركة نابع من ابتكار وإنتاج منتجات فريدة من نوعها تقوم بعمل أبحاث وتجارب عليها قبل بيعها في الأسواق المحلية و العالمية , ثم تقوم بتسويقها بأفضل الطرق والأساليب وذلك بعقد اتفاقيات مع شركات كبرى متخصصة تقوم لها بأعمال التسويق والادارة.

ولمعرفة المزيد عن تاريخ الشركة وتقدمها في السنوات السابقة إليكم التفاصيل الآتية :

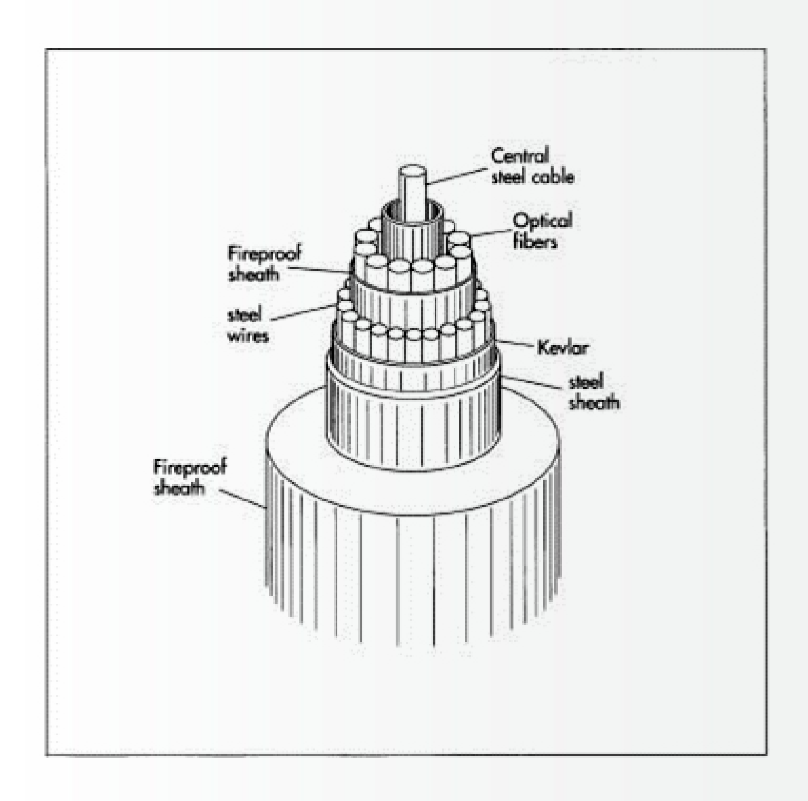
1) في عام 1990 قامت هواوي بعمل أبحاث وتسويق لتكنولوجيا الـ PBX , وكانت هذه التقنية أول تقنية استخدمتها, مستهدفة الفنادق والمنشآت الصغيرة.

2) في عام 1992 بعد تراكم المعرفة والموارد لدى هواوي عن هذه التكنولوجيا , قامت بتحقيق أول إنجاز لها بدخول سوق الاتصالات السلكية واللاسلكية , وذلك عندما انطلقت بإنتاج سويتشات الهاتف الرقمي من النوع C&C08 digital telephone switch) C&C08) , وكانت من أكبر السويتشات ذات الكفاءة والقدرة العالية الموجودة في الصين في ذلك الوقت , والتي كانت منتشرة في المدن الصغيرة والمناطق الريفية.

SDH



Optical fiber





4) في عام 1995 حققت مبيعات بلغتRMB1.5 مليار والتي هي أساساً مستمدة من الأسواق الريفية في الصين .
5) في عام 1997 توسعت هواوي دولياً خارج البلاد وذلك بعد فوزها بأول عقد لها , والتي كانت مع شركة Hutchison Whampoa في Hong Kong وكان بتوفير المنتجات لشبكات الـ fixed-line، وفي العام الذي يليه أطلقت منتجات ترتكز على تقنية لاسلكية من الجيل الثاني تسمى wireless GSM ثم توسعت إلى نهاية المطاف مقدمة تقنية الـ CDMA والـ UMTS في منتجاتها،(الـ GSM& CDMA& UMTS):هي تقنيات مستخدمة في عالم الـ mobile communications .

6) في عام 1999 افتتحت شركة للأبحاث العلمية والتنمية وذلك لتطوير الـsoftware الخاص بالاتصالات , وكان مقرها في عاصمة الهند في مدينة Bangalore .(نصيحة:ابحث وأقرأ عن هذه المدينة فهي ثالث أكبر مدينة هندية من حيث العدد السكاني (حوالي 6 مليون نسمة) , وهي في غاية الجمال من المعالم الموجودة بها كما , أنها تحتوي على 1500 شركة تكنولوجية , وتضم قرابة ٪40 من موظفي ميكروسوفت .
7) منذ عام 1998 وحتى عام 2003 تعاقدت هواوي مع شركة IBM لكي تقوم لها بأعمال الاستشارات الإدارية , وبعدها خضعت هواوي لتطور كبير في إدارة وتطوير هيكل وبناء المنتج الذي تقدمه .

المبيعات التي حققتها والموقف التنافسي

في الحقيقة تعتبر هواوي من أكبر الشركات التي لديها القدرة على التوسع في الأسواق الخارجية , كما أن مبيعاتها تتزايد بشكل تدريجي وملحوظ والدليل على ذلك:



2) في عام 2001 أطلقت أربع مراكز للبحث والتطوير في الولايات المتحدة , وانضمت للاتحاد الدولي للاتصالات , وفي عام 2002 وصلت مبيعاتها في السوق الدولية إلى 552 مليون دولار .

3) في عام 2004 واصلت توسعها في الخارج بعقد لبناء شبكة محمول من الجيل الثالث بشركة في هولندا , وبلغت قيمة هذا العقد أكثر من 25 مليون دولار أمريكي , وكان هذا أول عقد لبناء شركة في أوروبا .

4) في عام 2006 بلغت مبيعاتها حوالي 11 مليار دولار أمريكي (زيادة34 ٪ عن عام 2005) وكان 65 ٪ منها من الأسواق الخارجية , وبحلول نهاية عام 2008 قفزت المبيعات العالمية لأكبرشركة اتصالات في الصين إلى 46 في المائة , أي 23.3 مليار دولار أمريكي حتى وصلت إلى 30 مليار دولار أمريكي في عام 2009.

5) وفي عام 2010 بلغت مبيعاتها ل 185.2 بليون يوان.

6) في نيسان(ابريل) 2011 أعلنت هواوي زيادة أرباحها بنسبة 30 ٪عن عام 2010 مع ارتفاع صافي الربح إلى مليار RMB23.76 ، وكل ذلك بفعل النمو الكبير لمنتجاتها في الأسواق الخارجية .
فنرى أنّه في كل عام تتقدم هواوي و تحقق الكثير والكثير من الأنجازات , وأنّها في تفوق دائم , وأنّها تنافس نفسها لتسويق منتجاتها لتزيد من مبيعاتها , وبالفعل نجحت في ذلك.

تحدثنا الكثير عن تاريخ الشركة والمبيعات التي حققتها , ولكن لم نعرف ما المنتجات والشهادات التي تقوم بتقديمها شركة هواوي , فالكل يعتقد أنّ الشركة تقوم بإنتاج راوترات وسويتشات فقط , وأنّها منافسة لشركة سيسكو وجونيبر وغيرهم وأنا أيضاً اعتقدت ذلك وغافل عن المنتجات, الأخرى التي تقوم بإنتاجها , فهي تقوم بإنتاج منتجات متعددة تحقق من وراءها مبيعات هائلة

وبسبب تعدد هذه المنتجات قسمت هواوي منتجاتها لثلاثة أقسام وهي كالتالي:

1 -القسم الخاص بمنتجات الcloud : وتشمل الـ Software & Application والـ & Storage Network Security والـOSS وهي الحلول التي تقدمها هواوي.

2 -قسم الـPipe : و به المنتجات الخاصة بالـ Radio Access و الـFixed Access والـ Site Products والـ Transport NetworkوالـData Communication والـ Core Network.

3 - المنتجات الخاصة بالـdevices وتشمل الـ Personal Devices والـ Home Devices وللـ Enterprise.

وللتعرف على كل هذه المنتجات نحتاج الكثير من الشرح , لأن كل قسم منها له منتجات فرعية خاصة به , فمثلاً يوجد في قسم الـcloud الجزء الخاص بالـSecurity & Storage , وهذا الجزء يتحدث عن أجهزة الحماية والتخزين فبالتالي يوجد منتجات وأجهزة للحماية كأجهزة الـSAN (Storage Area Network) , والـ NAS (Network Attached Storage) , والـSwitch SNS وكل منتج منهم يحتاج لتفاصيل للتحدث عنه. فتخيلوا معي كم منتج تقوم الشركة بإنتاجه بعد معرفة كل المنتجات والأجهزة الفرعية الموجودة في كل قسم من الأقسام الثلاثة.ولكثرة المنتجات التي تقوم الشركة بإنتاجها فسوف نتحدث اليوم فقط عن القسم الخاص بالـ devices , و إن أردتم التعرف على باقي الأقسام ومنتجاتها الفرعية سأتطرق إليها في مواضيع أخرى إن شاء اللّه.

والآن إليكم بعض التفاصيل لكي تعرفوا أكثر عن الـ devices وأنوعها التي تقدمها هذه الشركة .

ما هي منتجات الـ devices التي تقدمها هواوي؟

في الحقيقة فإن شركة هواوي لا تهتم فقط بأجهزة الهاردوير الخاصة بالشبكات كالروترات والسويتشات كما ذكرنا , وإنما تقوم بإنتاج منتجات أخرى كأجهزة الهواتف الشخصية , مثل الـ Smart Phones والـ Feature Phones



Feature Phones

Smart Phones

وأيضاً تقوم بإنتاج أجهزة منزلية مثل الـ: Tablets،Broadband Modems،Gateways،Set-top Boxes،Fixed Wireless Terminals،Digital Photo Frames



Broadband Modems

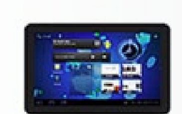
Gateways

Fixed-Wirless Terminals

Digital Photo Frames



Set-top boxes



Tablets

كما أنها تقوم بإنتاج منتجات لـ enterprise , وهذا هو محل اهتمامنا , وهذه قائمة بالمنتجات التي تقدمها في الـ enterprise.

A list of products	
Routers	Switches
Security	WDM
MSTP	IP Microwave
Integrated Access	Network Management
Radio Network Access	Unified Communications
Contact Center	Video Communications
Server	

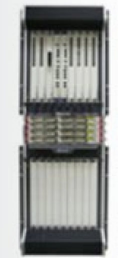
منتجات الـ Routers

فهي تقوم بإنتاج ثلاث فئات من الراوتر وهم : (NE Routers وMSCG وAR Routers).
وتتضمن فئة الـ (NE Routers) : الثلاث نماذج (موديلات) الآتية (NE5000E Cluster Router و NE40E Universal Service Router وNE20E & NE20 Series Multi-service Router).
وكل نموذج (موديل) له مميزات خاصة به , فالـNE5000E Cluster Router) (module يعتبر الـ (super core router) أي من الروترات الفائقة والأساسية التي تصنعها هواوي , لأنّه يستخدم في internet backbone , ويوجد منه نوعين : إما single chassis وmultiple chassis وهذا النوع يستخدم في عملية الـ Cluster.
كما أن هذا النموذج (الموديل) يدعم الـRouting protocol الآتية :
(IPv4 static route, OSPF, IS-IS, BGP-4, PIM, MSDP, MBGP) وله الكثير من المميزات مبيّنة في الجدول التالي :

Attribute	Description
Throughput capability	Non-block switch fabric, support multi Chassis The maximum bidirectional interface capacity: 200Tbps/64 Chassis
Switching performance	6.4Tbps/ single Chassis
Slots/CLC	16 slots/ single Chassis
Interface Types	GE, 10GE, OC768c POS, 100GE, etc.
Routing protocol	IPv4 static route, OSPF, IS-IS, BGP-4, PIM, MSDP, MBGP
IPv6	IPv4 & IPv6 dual stack; ipv6 line speed forwarding based on hardware IPv6 static route, BGP4+, RIPng, OSPFv3, IS-ISv6 IPv6 peer discovery, PMTU discovery, TCP6, ping IPv6, Tracert IPv6, socket IPv6, TFTP IPv6 client, IPv6 policy route , IPv6 NetStream, etc Manually configured tunnel, automatic tunnel, 6 to 4 tunnel
High Availability	1:1 standby for MPU, 3+1 backup switching fabric, 1+1 backup for power supply and fan hot swappable based on state Non-stop Forwarding (NSF), and Non-stop Routing (NSR) BFD for VRRP/BGP/OSPF/ISIS/TE LSP/LDP/ LSP/TE and PIM IGP/BGP/Multicast Fast Convergence IP/LDP/BGP/TE Fast Re-Route (FRR), BGP/ISIS Auto FRR, ETH Trunk, IP Trunk ; In-Service Software Upgrade (ISSU), Automatic fault diagnosis function, Hot Patching Configuration Management Bi-Direction Compatible

أما النموذج (الموديل) (NE40E Universal Service Router) : فهو من المنتجات الراقية التي تقدمها شركة هواوي , فهو يدعم العديد من الخدمات المتقدمة مثل :
(multicast ,MPLS,IPv6,QoS, (L2VPN, L3VPN, multicast VPN (MVPN)

أما النموذج (الموديل) الأخير (NE20E & NE20 Series Multi-service Router) : فهو يجمع بين خدمات عديدة توجد في الموديلات السابقة , ولكن له 4 series خاصة به وهم : (NE20-8, NE20-4 NE20-2 and NE20E-8.



Single chassis



Back to back cluster

NE5000E Cluster Router



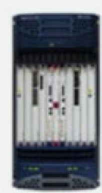
NE40E-X16



NE40E-X8



NE40-EX3

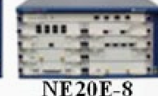


NE40E-8

NE40E Universal Service Router



NE20E-8



NE20E-8



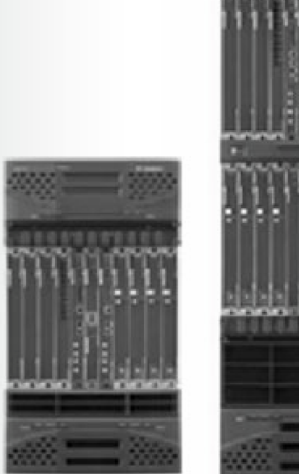
NE20E-4



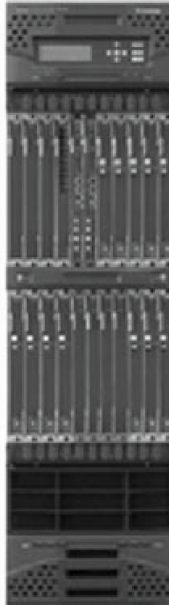
NE20E-2

NE20E & NE20 Series Multi-service Router

أما فئة الـ (MSCG) تتضمن5 موديلات وهم : (ME60-8, ME60-16, ME60-X3, ME60-X8 and ME60-X16).



ME60=8



ME60=16

ME60=X3

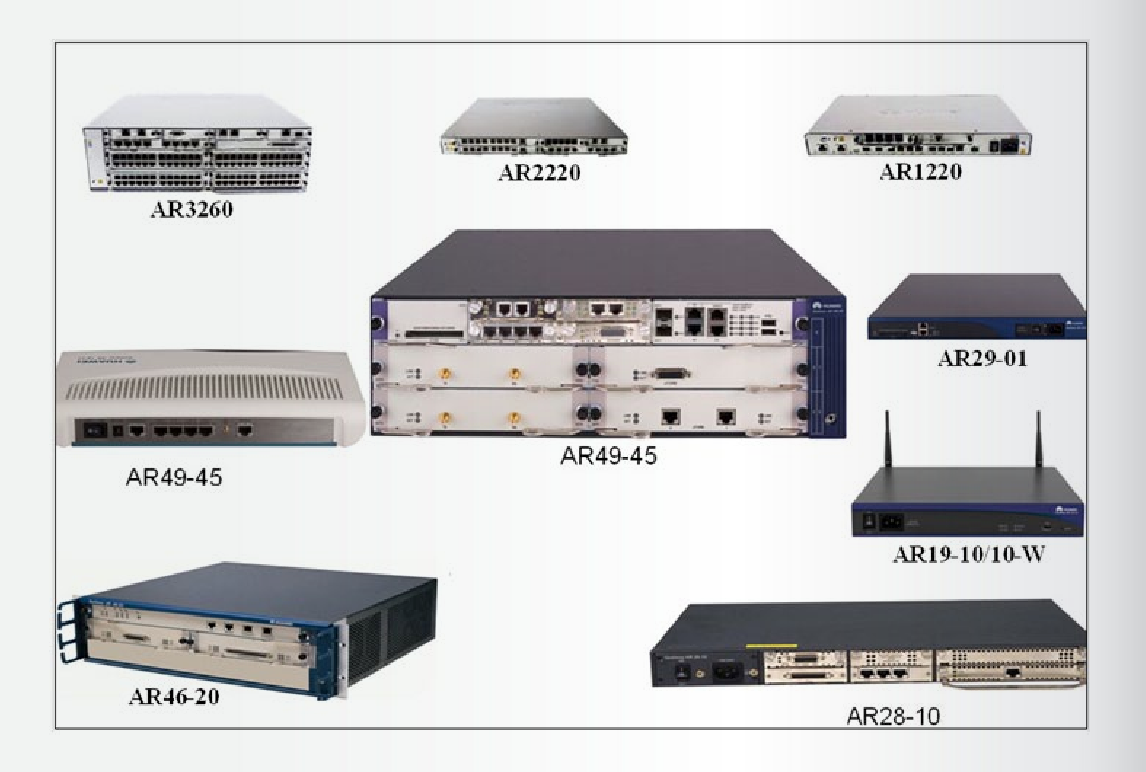


ME60=X8



ME60=X16

وتتضمن فئة الـ 9) AR Routers موديلات وهم : (AR3200 seires enterprise routers و AR2200 seires enterprise routers و AR1200 seires enterprise routers و Quidway AR49 series routers و Quidway AR29 series routers و Quidway AR19 series routers و Quidway AR46 series routers و Quidway AR28 series routers و Quidway AR18 series routers)



وهذه الفئة يوجد بها روترات تستخدم في الشركات الكبيرة - enterprise - مثل : (, AR1200 seires ,(AR2200 seires AR3200 seires enterprise.

ويوجد منها للشركات المتوسطة والصغيرة والتي تقدم خدمات عديدة مثل :
AR19 series, Quidway AR49 series, Quidway AR46 series ,Quidway AR28 series, Quidway) (AR29 series

ويوجد منها للمكاتب والمنازل مثل : (Quidway AR18 series).

ولمعرفة مميزات ومواصفات أي موديل من أي فئة من الفئات الثلاثة اضغط فقط على الموديل الذي ترغب معرفته من هنا (NE5000E Cluster Router /NE40E Universal Service Router/NE20E & NE20 Series Multi-service Router / Huawei ME60 Series Multi-Services Control) Gateway AR3200 seires enterprise routers / AR2200 seires enterprise routers / AR1200 seires enterprise routers / Quidway AR49 series routers / Quidway AR29 series routers / Quidway AR19 series routers / / (Quidway AR46 series routers / Quidway AR28 series routers / Quidway AR18 series routers وسوف يظهر لك كل مميزاته ومعلوماته.

منتجات الـ Switches

هناك 7 نماذج (موديلات) للسويتش , وكل موديل له series خاص بها , وموديلات السويتش هي : (S9300 Terabit Routing Switchesو S7700 Series Smarter Routing Switchesو S6700 Series 10G Switchesو S5700 Series Gigabit Enterprise Switchesو S3700 Series Enterprise Switchesو S2700 Series Enterprise Switchesو S1700 Series Enterprise Switches)



المنتجات التي توجد في مجال الـ security هي الـ Firewall & Unified Threat Management وتشمل3 منتجات وهي : (Eudemon 200E-X Series Productsو Eudemon 1000E-X Series Productsو Eudemon 8000E-X Series Products)



ولمعرفة التفاصيل عن هذه المنتجات التي تقدمها هواوي , فإليكم هذا المرجع
Huawei Data.com

نسخة التشغيل المستخدمة في روترات Huawei

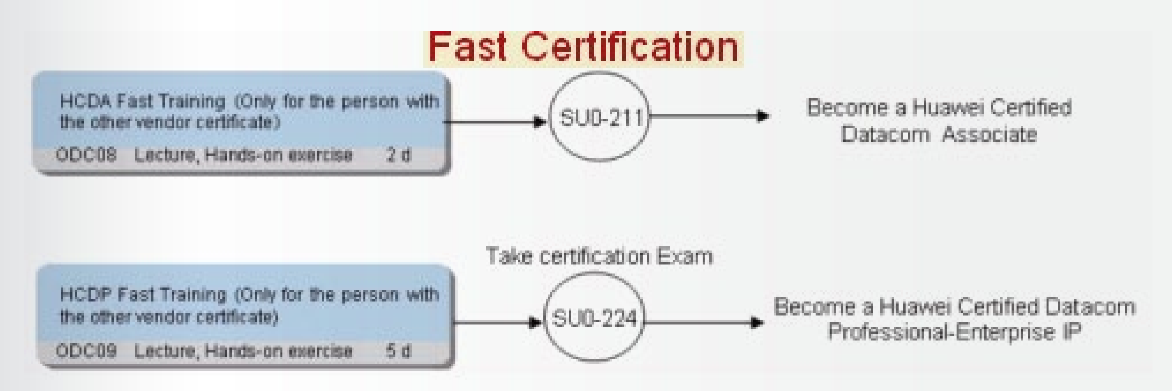
يعتبر نظام التشغيل VRP فاكهة هواوي , لأنّها اكتسبت لسنوات كثيرة من الخبرة , في مجال الشبكات تقوم بعمل أبحاث لكي تقوم بتصميمه حتى يعمل على منتجات الشبكات الخاصة بها من ((Router & Switch فهو نظام تشغيل ملك وخاص لها , ويعمل فقط علي منتجاتها , ويسمى Versatile أي أنّه متعدد الاستعمال لأنّه يعمل على أي Seriesمن الراوتر أو السويتش فهي تستخدم O.S واحدة لكل الـplatform التي لديها.
ومن مميزاته : أنّه يعد من أفضل الـ OS التي يوجد بها تكامل حقيقي في الوقت الحالي , فهو مصمم لكي يعمل ويتوافق مع الشبكات التي يوجد بها تصميم متقدم ومستمر وتستطيع تطويره , أي أ نّه يتمتع بالمرونة العالية والموثوقية و تستطيع إدارته في شبكتك بكل سهولة , كما تستطيع بنائه في شبكتك من البداية إلى النهاية وأنت مطمئن , لأنّه يتمتع بالكفاءة والحماية العالية (secure network of high efficiency) , ويدعم الكثير من البروتوكولات ومزود بآليات إدارة من أجل (Unicast and Multicast routing algorithms). لذلك فإنّ الـplatform الخاص بهواوي تدعم Routing protocols تعمل على أي layer طبقاً للمعدات والأجهزة الموجودة في الـ network.
وعندما قامت هواوي بتصميم نظام التشغيل VRP راعت الحماية والحفاظ على مصادر مستخدميها بشكل كامل لكي تضمن له الموثوقية والكفاءة العالية والسيكورتي في الشبكة , وذلك بتزويد عدد كبير من البروتوكولات الخاصة بالـ security والـ backup , وشملت عمليات الـ access control, authentication, firewall,) encapsulation encryption, log function, backup center function, route backup, and load balancing).
أما في عملية الـ configuration فالـVRP يقدم لك مرونة عالية في إدارة الشبكة , و أوامره تكون شبيهة بالأوامر المستخدمة في الـweb والـ SNMP والتي تكون على شكل command line.
وأيضاً تستطيع عمل configuration والدخول remotely على راوتر هواوي من خلال الـtelnet أو عن طريق الـdial up بالمودم .
ولمزيد من المعرفة عن نظام التشغيل اضغط على الرابط الأتي :
Huawei's Versatile Routing Platform (VRP)

ماهى الشهادات التي تقدمها Huawei ؟

كثير منّا يتجه نحو شهادات ميكروسوفت وسيسكو ولا يهتم بالشهادات التي تقدمها هواوي نظراً لعدم معرفتنا بها أو عدم احتكاكنا في سوق العمل بأي من منتجات هواوي , في الحقيقة قامت الشركة بتقديم مجموعة من الشهادات لدارسيها و وضعت لك طريقين لأخذ هذه الشهادات , فإمّا أن تبدأ مسارك بالـ Fast Certification أوالـ Career Certification , وكلاً من المسارين له 3 مراحل , لكي تصبح من الخبراء فهي تبدأ بمستوى الـ Associate ويسمى ((HCDA , ثم إلى مرحلة الـ Professional ويسمى (HCDP) وأخيراً إلى مستوى الخبراء وهو (HCDE).



مسار الـ Fast Certification: يسمح للموظفين ذوي الخبرة المرتبطة بالعمل بمنتجات هواوي أن يحصلوا على الشهادة في أقصر وقت ممكن.



ومسار الـ Career Certification: تجعلك (IP technical) أي فني متخصص وكفء للعمل في شركات الاتصالات والمؤسسات التي بها منتجات هواوي . ولها طريقين
(Carrier ip و enterprise ip) فالفرق بينهم هو اختلاف الامتحانات في مستوى الـ professional.

a.Carrier IP Certification

HCDA-HNTD (Huawei Certified Datacom Associate-Huawei Networking Technologies and Device) Training
ODC01 Lecture, Hands-on exercise 8 d
SU0-211
Become a Huawei Certified Datacom Associate

Take certification Exam
HCDP-BCAN (Huawei Certified Datacom Professional-Building Carrier Access Network) Training
ODC03 Lecture, Hands-on exercise 6 d
SU0-121

Take certification Exam
HCDP-BCRN (Huawei Certified Datacom Professional-Building Carrier Routing Network) Training
ODC02 Lecture, Hands-on exercise 9 d
SU0-122

Take certification Exam
HCDP-BITN (Huawei Certified Datacom Professional-Building IP Telecom Network) Training
ODC04 Lecture, Hands-on exercise 7 d
SU0-123

Become a Huawei Certified Datacom Professional-Carrier IP

b. Enterprise IP Certification

HCDA-HNTD (Huawei Certified Datacom Associate-Huawei Networking Technologies and Device) Training
ODC01 Lecture, Hands-on exercise 8 d
SU0-211
Become a Huawei Certified Datacom Associate

Take certification Exam
HCDP-IERN (Huawei Certified Datacom Professional-Implementing Enterprise Routing Network) Training
ODC05 Lecture, Hands-on exercise 7 d
SU0-221

Take certification Exam
HCDP-IESN (Huawei Certified Datacom Professional-Implementing Enterprise Switching Network) Training
ODC06 Lecture, Hands-on exercise 7 d
SU0-222

Take certification Exam
HCDP-IENP (Huawei Certified Datacom Improving Enterprise Network Performance) Training
ODC07 Lecture, Hands-on exercise 5 d
SU0-223

Become a Huawei Certified Datacom Professional-Enterprise IP

ولمعرفة ما المحتويات التى تقدمها كل شهادة والوقت الخاص بكل امتحان , اتبع الرابط التالي :
http://www.huawei.com/enterprise/certification-exam-outlines.do

ولمعرفة أسعار وأكواد الامتحانات فأنظر للجدول التالي :

Certification	Code	Programs	Exam Fees
HCDA	SU0-211	HCDA-HNTD Huawei Certified Datacom Associate - Huawei Networking Technology and Device	150 USD
HCDP-Carrier IP	SU0-121	HCDP-BCAN Huawei Certified Datacom Professional - Building Carrier Access Network	120 USD
	SU0-122	HCDP-BCRN Huawei Certified Datacom Professional - Building Carrier Routing Network	120 USD
	SU0-123	HCDP-BITN Huawei Certified Datacom Professional - Building IP Telecom Network	120 USD
HCDP-Enterprise IP	SU0-221	HCDP-IERN Huawei Certified Datacom Professional- Implement Enterprise Routing Network	105 USD
	SU0-222	HCDP-IESN Huawei Certified Datacom Professional- Implement Enterprise Switching Network	105 USD
	SU0-223	HCDP-IENP Huawei Certified Datacom Professional- Improving Enterprise Network Performance	105 USD
	SU0-224	HCDP Fast Certification （For Enterprise IP）	150 USD

واخيرا اليكم هذه الروابط:
الموقع الرسمى بالأنجليزية لهواوي :
/http://www.huawei.com/en

لمعرفة آخر الإخبار عن هواوي باللغة العربية :
http://www.huawei.com/ar/catalog.do?id=744

قناة هواوي على الـ youtube: http://www.youtube.com/user/
HuaweiDeviceCo?blend=7&ob=5

وفي النهاية أتمنى أن يكون الموضوع قد نال إعجابكم , وفي لقاء قادم إن شاء الله

طبولوجيات أو أنماط شبكات الواي فاي

WI-FI Topologies

لمحة عن الكاتب

نادر المنسي

الجنسية : مصر / مقيم بالكويت

مهندس اتصالات يطمح و يساعد في الرقي بالمحتوي العربي للشبكات عبر ترجمة و اعداد مقالات و كتب علمية

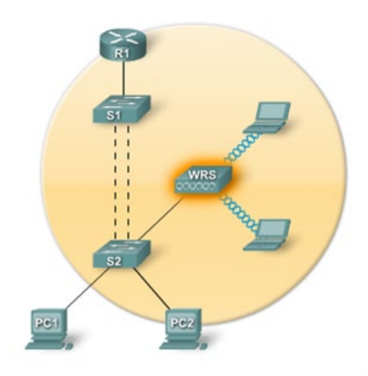
naderelmansi@gmail.com

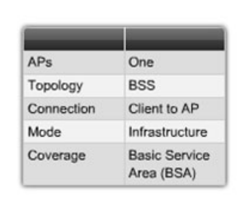
عند بداية دراستنا للشبكات السلكية عرفنا الفرق بين نوعي الكابلات straight, cross over , حيث تستخدم كابلات cross over للربط بين جهازين peer to peer بينما يتم استخدام straight cable للربط بين الحاسب و السويتش وهو ما يسمى بالبنية النجمية Star .

هذان أيضاً متوفران في الشبكات اللاسلكية .. لا أقصد طبعاً نوعي الكابلات ولكن نوعي الشبكات مع اختلاف في المسميات , فيتم تسمية الشبكات peer to peer بـ Ad hoc , بينما يتم تسمية الشبكة التي يستخدم فيها جهاز مركزي لتوصيل أكثر من جهاز حاسب بـ infrastructure.

و يوجد نمط جديد – إن صحت تسميته نمط - يجمع ما بين الاثنين اسمه WIFI-Direct أطلق حديثاً في سنة 2010 من جهة مؤسسة الواي فاي .

Network Infrastructure Mode



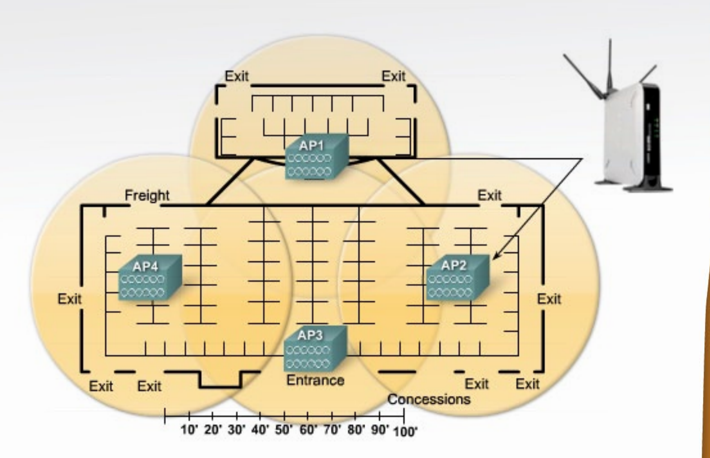


APs	One
Topology	BSS
Connection	Client to AP
Mode	Infrastructure
Coverage	Basic Service Area (BSA)

تعتبر عدم المركزية في اتخاذ القرارات و معالجة العمليات في الشبكة نقطة ضعف خطيرة و لذلك فإنّ كل الشبكات الحديثة و الواقعية تستخدم نظام مركزي يتم به التحكم في الشبكة و ربطها و ذلك عن طريق أجهزة الشبكة كالراوترات و السويتشات أو عن طريق خدمات مركزية موجودة على سيرفر رئيسي كخدمات قواعد البيانات المركزية أو التوزيع المركزي لأرقام الشبكة DHCP.

و لم تكن الشبكات اللاسلكية بعيدة عن هذا الواقع , بالرغم من أنّ الأجهزة اللاسلكية قادرة الاتصال ببعضها البعض دون وجود وسيط AD-HOC إلّا أنّها مفتقرة للأمن و التوسع في عدد الأجهزة و غيرها من الميزات التي توجد في الشبكات المركزية ,

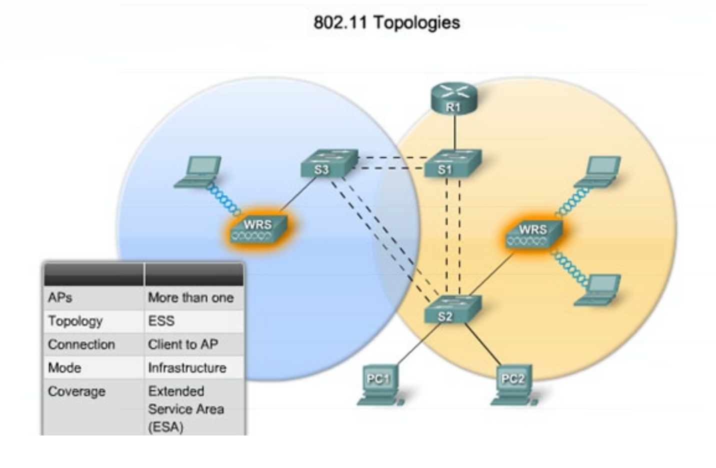
و لا يعتبر الأكسس بوينت هو الجهاز المركزي الوحيد المستخدم في الشبكات اللاسلكية , و لنكن واضحين أكثر فإن الجهاز الذي سيستخدم لعمل هذه المركزية سواء أكان أكسس بوينت أو غيره سيسمى Infrastructure Device , و أما الأجهزة التي ستتصل بهذا الجهاز فستسمى station STA , و لذلك فإنّ الأجهزة التي ستعتمد على وجود جهاز مركزي فإنها ستقع في ذلك الحيز الذي يجمعها به والذي سيسمى بمنطقة البث BSA Basic Service Area أو الخلية اللاسلكية Wireless Cell و هي دائرية كما بالشكل :



في الشبكات اللّاسلكية يعمل الأكسس بوينت كنقطة مركزية لاتصال الأجهزة لاسلكياً مثلما يعمل الـ Hub و الجسر Bridge في الشبكة العادية , فهو يتشابه مع الـ Hub في كونه لا يستطيع الإرسال و الاستقبال في نفس الوقت ,حيث أنه يرسل بنمط Half Duplex أو بمعنى لاسلكي يحتوي على مسار راديوي واحد فقط يرسل و يستقبل عليه ,

و يتشابه مع الجسر في أنه يرسل و يستقبل اعتماداً على العنوان الفيزيائي للجهاز MAC Address و يختلف معه في أن الفريم اللاسلكي أكثر تعقيداً من مثيلاتها في الشبكات السلكية , حيث يتكون الفريم المرسل في شبكات الإيثرنت من جزئين فقط هما : العنوان الفيزيائي للمرسل source MAC address و العنوان الفيزيائي للمستقبل destination MAC address , أما في الشبكات اللّاسلكية فيتكون الفريم اللّاسلكي من ثلاث أو أربع أجزاء ,الأول عنوان المرسل و الثانية عنوان المستقبل و الثالثة عنوان الأكسس بوينت و الرابعة هي العنوان الفيزيائي لجهاز الجسر اللاسلكي workgroup bridge المستخدم أحياناً في شبكات سيسكو و سنتكلم عنه يوماً ما .

و من ميزات هذا النمط أنّه قادر على التمدد باستخدام أكثر من أكسس بوينت و تسمى هذه الشبكة بـالشبكة الممتدة extended service set ESS



APs	More than one
Topology	ESS
Connection	Client to AP
Mode	Infrastructure
Coverage	Extended Service Area (ESA)

و هذه الشبكة يتم في كل أجهزتها استخدام اسم واحد فقط للشبكة SSID لتستطيع كافة الأجهزة الاتصال عبر أي جهاز من أجهزة الأكسس بوينت الموجودة ,

كما تحتاج أيضاً أن يكون هناك تداخل بين خلايا أجهزة الأكسس بوينت كما بالشكل كي لايكون هناك مناطق ميتة Dead Zone لا تستطيع الإشارة الوصول إليها , يتم ضبط كل خلية في الشبكة اللّاسلكية الممتدة على قناة ترددية Channel مختلفة عن جارتها كي لا يحدث تداخل بين أجهزة الأكسس بوينت , و يعطي معيار 802.11 b , ثلاث ترددات ممكنة للنشر بين هذه الخلايا .

WiFi-Direct Network

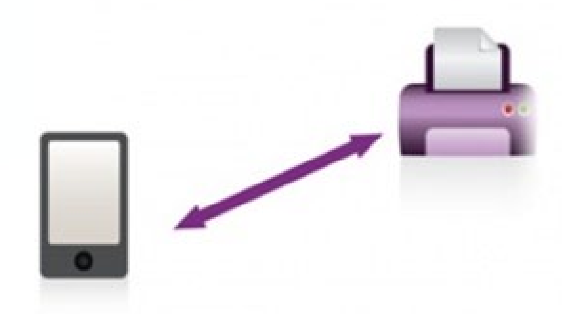


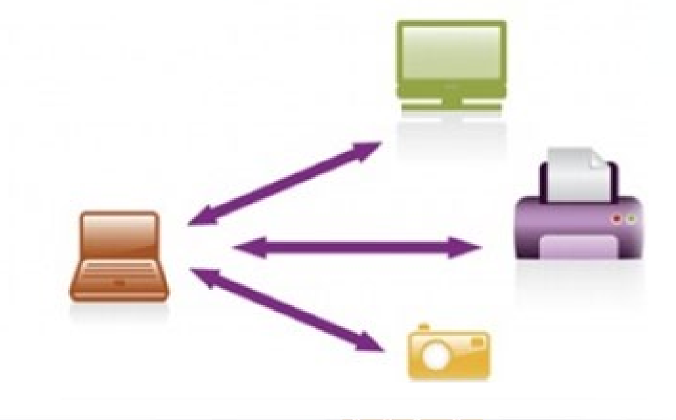
تعتبر هذه التقنية حديثة جداً – تقريباً في 2010 - و من أحد إصدارات مؤسسة الواي فاي , وهي تتشابه قليلاً في الشكل العام مع تقنية Ad hoc و لكنّها تختلف في المضمون معها و على العكس تتشابه في المضمون مع شبكات Infrastructure و تختلف معها في الشكل .

الأجهزة التي تدعم هذه التقنية تستطيع الاتصال فيما بينها طبقاً لوجود مكون إضافي بها و هذا المكون ليس هاردوير بل سوفت وير يسمى «soft Access Point» أي أنّ الجهاز سواء كان موبايل أو كمبيوتر أو طابعة أو كاميرا يستطيع التعامل كأكسس بوينت و يتصل بأي جهاز آخر توجد به هذه الخاصية .

و تتميز أجهزة هذا النمط في أنّها تستطيع تأمين الاتصال عبر تقنية WPA2 و تم دمج تقنية WIFI Protected Setup معها لتحقيق التوثيق .

الأروع في هذه التقنية أنّ أجهزتها تستطيع الاتصال في نفس الوقت مع أكثر من جهاز أي أنّها تزيد على نمطي Ad-Hoc و Infrastructure في أنّها تتصل فيما بينها Full-Duplex مثلما تتصل أجهزة السويتشات و ليس الهب أو الأكسس بوينت .





كذلك فإنها قادرة على تحقيق الاتصال عبر ترددات 2.4 و 5 جيجا هرتز على بعد 200 متر و بسرعة بمقدار 250 ميجابت في الثانية , في حال دُعم الجهاز لمعايير تسمح بهذه السرعة مثل IEEE 802.n , فإن الأجهزة التي تدعم هذه التقنية قادرة على مشاركة الإنترنت للأجهزة المتصلة بها
يعتبر الجهاز المعجزة Galaxy S smartphone GT-I9000 أحد و أهم الأجهزة التي بدأت دعم هذه التقنية في نوفمبر 2010 , أي بعد أشهر قليلة من إطلاق الواي فاي لهذه التقنية .

و لكي تتأكد من دعم الجهاز لهذه التقنية فابحث عن هذا اللوجو



لمحة عن الكاتب

أنس المبروكي

الجنسية : المغرب

23 سنة، مهندس في الشبكات والأنظمة (EMSI- Rabat)

CCNA R&S ,CCNP R&S

mabroukianas@gmail.com

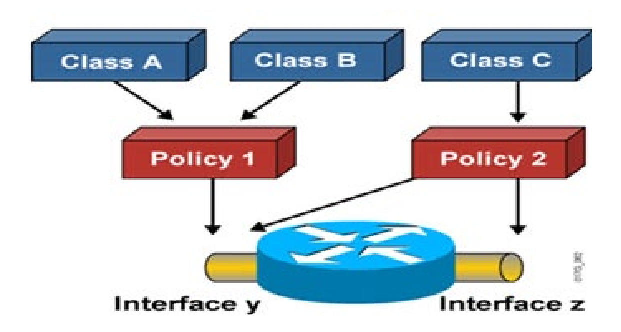
كيفية إعداد الـ QoS على أجهزة سيسكو

بعد تعرفنا في العدد السابق على أساسيات تقنية الـ QoS , سأحاول في هذا المقال كما وعدتكم في خاتمة الجزء الأول توضيح كيفية إعداد الـ QoS على أجهزة سيسكو مع بعض الأمثلة ، كما سنتعرف على عدة معلومات متقدمة حول الـ QoS ، تشمل إدارة ازدحام الترافيك (Congestion management) ، تجنب ازدحام الترافيك (Congestion avoidance) ، الـ Traffic Policing ، الـ Traffic shaping ، و فعالية اللينك (Link efficiency).

1.طرق إعداد الـ QoS على أجهزة سيسكو :

1.1: Cisco Modular QoS CLI .

تتّبع الـ MQC ثلاث خطوات لتنفيذ الـ QoS في الشبكة .أولاً يتم تعريف كل فئة (Class)من الترافيك فيClass-map , ثانياً تحديد سياسات الـ QoS أي Qos policies وربطها بفئات الترافيك المحددة في الخطوة الأولى ، أخيراً ربط الـQoS policies بالـinterfaces .



تحديد فئات الترافيك ، تحديد الـPolicies و تطبيق الـPolicies على الـ Interfaces

- Class Maps : ما هو الترافيك المهتم به ؟

تحتوي الـ Traffic class على ثلاثة عناصر رئيسية : اسم (case-sensitive name) ، سلسلة من أوامر match و إذا كان هناك أكثر من أمر match في الترافيك class،نضيف تعليمات بشأن كيفية تقييم هذه الأوامر . تعمل الـTraffic map في وضعين مختلفين :

Match all - : يجب اكتمال جميع الشروط وهو Default Mode .

Match any :- على الأقل يجب أن يحترم شرط واحد.

- Policy Maps : ماذا سنفعل بهذا الترافيك ؟

تحتوي الـTraffic policy على ثلاثة عناصر أساسية , وهي (case-sensitive name)،Traffic class والـQos policy المرتبطة بالـTraffic class .

MQC تدعم الـ Qos mechanisms التالية , وسنشرح هذه الـ Mechanismsفي الفقرة الثانية إن شاء اللّه :

- (Class-based weighted fair queuing (CBWFQ
- Low-latency queuing
- Class-based policing
- Class-based shaping
- Class-based marking

- Service Policy : أين سنضع هذه الـ policy؟

يمكن تطبيق الـ Service policy على الـ interface inbound packets أوالـ interface outbound packets .

يوضح الرسم التالي الأوامر اللّازمة لإعداد الـ MQC QoSأثناء كل خطوة.

Classification Configuration

Class-map myclass1
(matching parameters follow ...)
Class-map myclass2
(matching parameters follow ...)

Action/PHB Configuration

Policy-map mypolicy
class myclass1
(Actions/PHB's FOR THIS CLASS follow: marking, queuing, etc.)
class myclass2
(Actions/PHB's FOR THIS CLASS follow: marking, queuing, etc.)

Enable on Interface

Interface S 0/0
service-policy output mypolicy

في المثال التالي قمنا بتصنيف ترافيك البريد الإلكتروني (SMTP, IMAP, POP3) في class map ، ثم وضع بروتوكول KaZaa ، الذي يستخدم لتحميل الموسيقى في class map ثانية. Voice traffic وضع في class map أخرى . بعد ذلك تمنح الـ Policy الـ Bandwidth اللاّزمة لكل نوع من الترافيك .

```
Router(config)#class-map match-any EMAIL
Router(config-cmap)#match protocol pop3
Router(config-cmap)#match protocol imap
Router(config-cmap)#match protocol smtp
Router(config-cmap)#exit
Router(config)#class-map MUSIC
Router(config-cmap)#match protocol kazaa2
Router(config-cmap)#exit
Router(config)#class-map VOICE
Router(config-cmap)#match protocol rtp
Router(config-cmap)#exit
Router(config)#policy-map QOS-STUDY
Router(config-pmap)#class EMAIL
Router(config-pmap-c)#bandwidth 128
Router(config-pmap-c)#exit
Router(config-pmap)#class MUSIC
Router(config-pmap-c)#police 32000
Router(config-pmap-c)#exit
Router(config-pmap)#class-map VOICE
Router(config-pmap-c)#priority 256
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#interface serial 0/1
Router(config-if)#service-policy output QOS-STUDY
```

لاحظ أنّ الـ policy-map QOS-STUDY أعطت 128 كيلوبايت لترافيك البريد الإلكتروني. لكن ، الـ Bandwidth الممنوحة لبروتوكول Kazaa v2 محصورة في 32 كيلوبايت. الـ voice Packets لديها Bandwidth تعادل 256 كيلوبت في الثانية بالإضافة إلى «أولوية» في المعاملة ، وهذا يعني أنّه يتم إرسالها أولاً (قبل أي ترافيك آخر) في حدود 256 كيلوبت في الثانية .

السؤال المنطقي التالي هو : «ماذا يحدث لجميع الترافيك التي لم تصنّف ؟ يقوم الـ IOS بإنشاء class-default class-map، و التي تصنّف أي ترافيك غير مصنّف من قِبل الـ class maps المحددة. أخيراً، في المثال السابق ،فإنّ الـ policy-map تطبق في اتجاه الـ Outbound على الـ Serial 0/1 interface .

و يمكن استخدام الأوامر التالية لعرض المشاكل و التحقق من عمل الـ MQC :

```
Router#show class-map [class-map-name]
Router#show policy-map [policy-map-name]
Router#show policy-map interface interface-identifier [input | output]
```

1.2: Cisco AutoQoS VoIP .

نحتاج إلى أمر واحد على الـInterafce لإعداد الـQos

AutoQoS

```
interface Serial0
        bandwidth 256
        ip address 10.1.61.1 255.255.255.0
        auto qos voip
```

الـAutoQoS VOIP مدعومة في series routers Cisco **1760**, **1800**, **2600** , **2800**, **3600**, **3700**, **3800**, **7200**
و Cisco Catalyst **2950**, **2960**, **2970**, **3550**, **3560**, **4500**, and **6500** series switches
يمكنك استخدام أمر show auto qos للتحقق من إعداد الـ VOIP AutoQoS .

1.3: Cisco AutoQoS Enterprise .

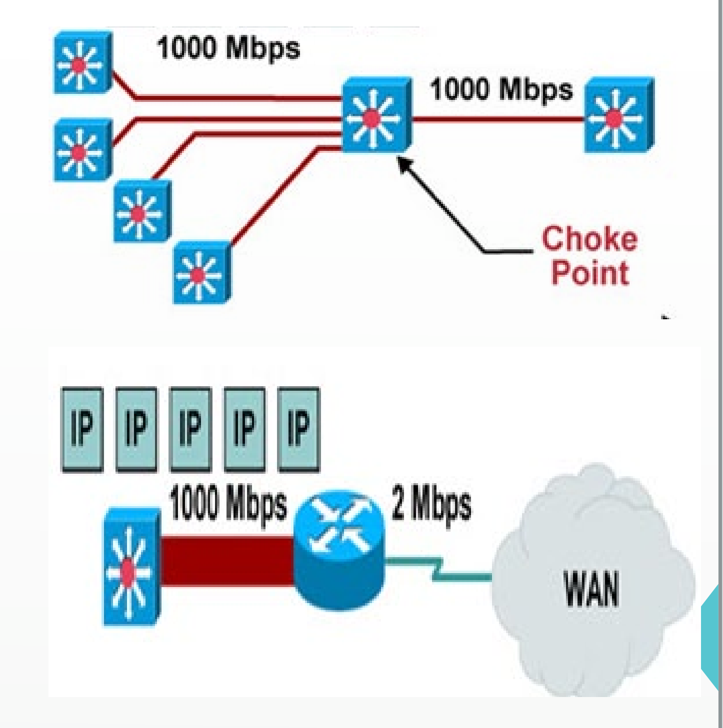
نحتاج إلى أمرين على الـWAN Interface .
auto discovery qos : تقوم بتجميع الإحصائيات عن الترافيك.
auto qos : هذا الأمر لن يُفعّل حتى يتم جمع الإحصائيات في المرحلة الأولى و يكون ذلك بعد يومان أو ثلاثة على الأقل . فهو يقوم بإنشاء الـ QoS policy بالاعتماد على الإحصائيات المجمعة وتفعيل الـservice policies على الـ Interface حيث تم إدخال الأمر.
توضح الصورة أسفله بعض إحصائيات الترافيك المجمعة عن طريق أمرauto discovery qos وذلك خلال يومان و 55 دقيقة.

```
Router#show auto discovery qos
 AutoQoS Discovery enabled for applications
 Discovery up time: 2 days, 55 minutes
 AutoQoS Class information:
  Class VoIP:
  Recommended Minimum Bandwidth: 517 Kbps/50% (PeakRate)
     Detected applications and data:
     Application/        AverageRate        PeakRate     Total
     Protocol            (kbps/%)           (kbps/%)     (bytes)
     rtp audio            76/7               517/50       703104
  Class Interactive Video:
  Recommended Minimum Bandwidth: 24 Kbps/2% (AverageRate)
     Detected applications and data:
     Application/        AverageRate        PeakRate      Total
     Protocol            (kbps/%)           (kbps/%)      (bytes)
     rtp video            24/2               5337/52       704574
  Class Transactional:
  Recommended Minimum Bandwidth: 0 Kbps/0% (AverageRate)
     Detected applications and data:
     Application/        AverageRate        PeakRate      Total
     Protocol            (kbps/%)           (kbps/%)      (bytes)
     citrix               36/3               74/7         30212
     sqlnet               12/1               7/<1         1540
```

2. Qos Mechanism :

2.1.إدارة ازدحام الترافيك (Congestion management) :

عند سماعك لمصطلح الـ congestion management ،فهذا يعني الـ queuing . هذه المصطلحات لها نفس المعنى , كما نعلم يمكن حدوثcongestion عند أي نقطة في الشبكة ويقع هذا الشيء عندما توجد نقط عدم تطابق السرعة (Speed msismatches) ، الـ aggregation ،لإدارة الـcongestion نستخدم الـ queuing وذلك لتوفير ضمانات لـ Bandwidth والـ Delays.



يوضح الرسمان أعلاه حدوث عملية الـ Speed mismatches والaggregation.

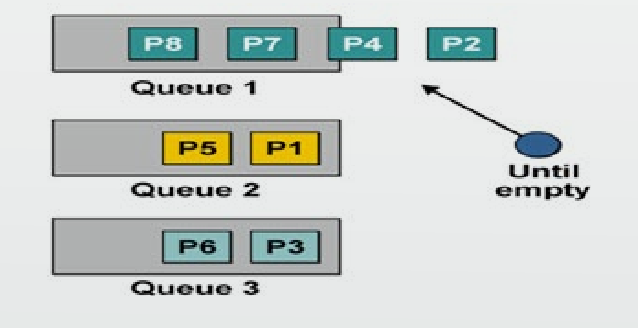
هناك خمسة خوارزميات (Algorithms) لـ Queuing :

 (FIFO(First IN First Out :

هو أبسط Algorithm يستعمل طابور (Queue) واحد ، الـ Packet الأولى التي تدخل هي الأولى التي تخرج.

 Priority Queuing :

يستخدم عدةQueues ويتيح تحديد الأولويات ، يقوم دائماً بإفراغ الـQueue الأول قبل الانتقال إلى الـQueue الموالي .في المثال أسفله يتم إفراغ الـ Queue 1 ،بعد ذلك ننتقل إلى الثاني ثم الثالث.



 Round Robin :

يستخدم عدةQueues ولا يتيح تحديد الأولويات، يفرغ Packet كل Queue ثم يكررالعملية.

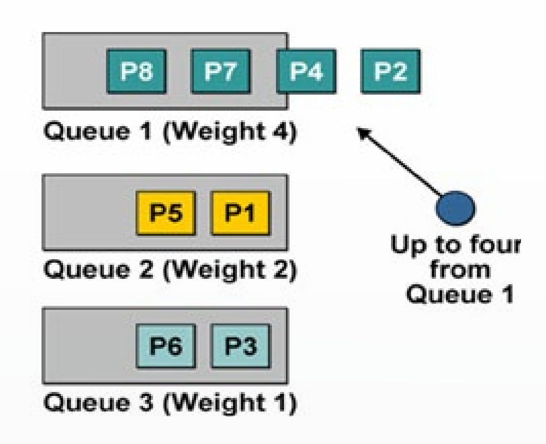
 Weighted Round Robin :

يتيح تحديد الأولويات، يعطىWeight لكلQueue . وبعد ذلك يتم إفراغ الـ Packet من الـ Queue حسب الـ Weight الممنوح . سنستعرض العملية في المثال التالي :

إرسال 4 packets من الـ1 Queue .

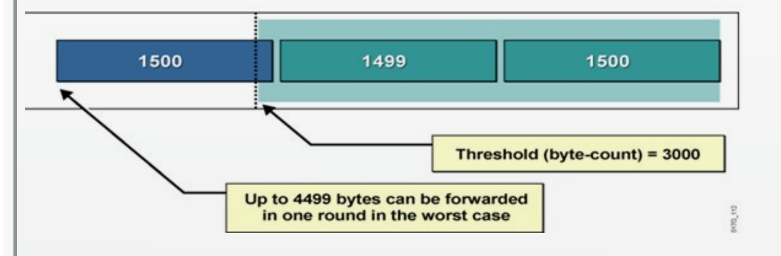
إرسال2 Packets من الـ2 Queue .

إرسال Packet واحدة من الـ3Queue . ثم العودة إلى الـ1 Queue .



بعض المشاكل قد تصادف عمل هذا الـ Algorithm لأن بعض تطبيقات الـ WRR ترسل عدد محدد من البايت من كلQueue ،إذن يمكن أن ترسل عدة Packets من كلQueue .

في هذا المثال العدد المحدد لإرسال (threshold) وهو 3000 بايت ، تتكون الـ Packets الأولى والثانية من 2999 بايت، إذن سيقوم الروتر بإرسال الـ Packet الموالية بأكملها رغم أنّ المجموع في هذه الحالة هو 4999 بايت , أكبر من العدد المحدد الذي هو 3000 .



 Deficit Round Robin :

اخترع هذا الـ Algorithm لمعالجة المشكلة السابقة ، فهو يقوم بتسجيل عدد البايتات الإضافية التي أرسلت من كلQueue ، يسمى هذا الشيء بالـ Deficitأو العجز , ويتم طرح هذا العدد من العدد المحدد في الدورة القادمة. في المثال السابق العدد المحدد لإرساله هو 3000 بايت، حجماً هو 1500، 1499 و 1500. إذن المجموع المرسل هو 4499 بايت. الـ Deficit في هذه الحالة هو(4499 – 3000) = 1499 ، في الدورة القادمة يرسل فقط .

(threshold – deficit)=(3000 -1499) = 1501

2.2. تجنب ازدحام الترافيك (Congestion avoidance) :

عملياً، يقوم الروتر بحذف الـ Packets القادمة إذا تم ملئ الـ Queue الخاص بالـ Interface بغض النظر عن الأولوية الممنوحة لـ Packets القادمة. لمنع حدوث هذه المشكلة نستخدم تقنية تسمى (RED) Random Early Detection, وهو يقوم بمراقبة الـ Traffic loads في الشبكة لمحاولة استباق وتفادي حدوث هذا الازدحام . ويتحقق هذا من خلال حذف الـ Packet.

2.3.Traffic Policing و Traffic shaping :

يمكن استخدام الـ Policing في اتجاه الـOtbound أو الـ Inbound. وعادة ما يحذف الـ Packets التي تتجاوز حد السرعة المعدة من قبل الأدمن , لأنّ الـ Policing يحذف الـ Packets، مما يؤدي إلى إعادة إرسالها، فمن المستحسن استخدامه في الـInterfaces التي لديها سرعة كبيرة.

الـ Shaping يمكن تطبيقه فقط في اتجاه الـ Outbound .بدلاً من حذف الترافيك الذي يتجاوز السرعة المحددة، يقوم بتأخير الترافيك ويضعها في الـ Buffer حتى تصبح الـ Bandwidth متوفرة. لهذا السبب فإنّ الـ Shaping يحافظ على الـ Bandwidth، بالمقارنة مع الـ Policing، على حساب زيادة التأخير(Delays). ولذلك، فمن المستحسن استخدامه في الـ Interface التي لديها سرعة بطيئة.

الـ Policing يحذف (drop) أو يعلم (mark) الـ Packets عندما يتم الوصول إلى الحد المسموح به. أما الـ Shaping فهو يقوم بـ queue لـ packets عندما يتم الوصول إلى الحد المسموح به.

2.4. فعالية الكابل (Link efficiency) :

لتحقيق أقصى استفادة من الـ Bandwidth المحدودة المتوفرة في الlinkات البطيئة، يمكنك استعمال الـ Compression أو الـ Link Fragmentation& Interleaving(LFI).

ضغط الـ Payload يستخدم أحد خوارزميات الضغط (compression algorithm) لضغط الـFrame payload .

ضغط الـ Haeders يخفض الـ Overhead عن طريق ضغط الـ IP header والـ Upper-layer header .

عملية الضغط تقوم بزيادة استهلاك الـ CPU وهذا يضيف الـ Delays. ولكن حجم الـ Packets يصغر يعني أنها تأخذ وقت قصير لإرسالها.

الـ LFI تعالج مسألة «delaysserialization» وهو الوقت اللّازم للـPackets للخروج من الـ Interfaces. على سبيل المثال : إرسال Data Packetكبيرة في لينك بطيء السرعة يمكنها زيادة الـ Delay بالنسبة لـ Voice Packet بسبب الوقت اللّازم لـ Data Packet للخروج من الـ Interface .

الـ LFI تقسم أو تقطع (fragments) الباكيت الكبيرة ويتم إرسال الـVoice packets الصغيرة بين القطع (fregments) الأخرى .وهذا يقوم بالحد من الـ delaysserialization الذي يواجه الـPackets الصغيرة.

الـ LFI يقلل من الـ Delays والـ Jitter بالنسبة للباكيت الصغيرة (بروتوكول الـ Voip) من خلال عملFragment للباكيت ذات الحجم الكبير للسماح للباكيت الصغيرة بالانتظار لوقت أقل.

بهذا نكون قد انتهينا من شرح هذه التقنية الرائعة , وقد حاولت جاهداً التحدث عن كل المفاهيم حول الـ QoS من خلال جزأين؛ جزء أول في العدد السابق وجزء ثاني في العدد الحالي. أتمنى أن أكون قد وفقت في الشرح وأضفت شيء للمحتوى العربي كما أتمنى أن القاكم في موضوع قريب إن شاء الله. حفظكم الله ورعاكم.







FritzBox

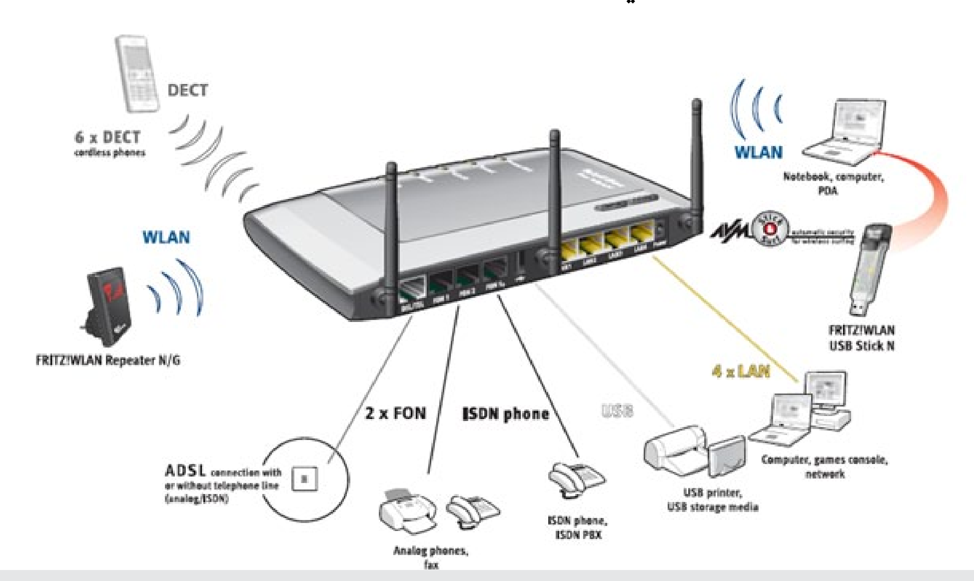
حديثي اليوم عن جهاز كثير الانتشار في أوروبا وذو خصائص مهمة ومميزة , يوفر لنا خدمات متكاملة في عالم الانترنت واتصالات الصوت عبر الانترنت VOIP , بالإضافة لكونه يقدم خدمات مشاركة ومركزية لأجهزة التخزين والطباعة بالإضافة لخدمات ربط تلفونات لاسلكية بالجهاز , وإمكانية تصفح البريد الإلكتروني من خلال جهاز الهاتف المنزلي , والكثير الكثير من المميزات , لنبدأ بالتفاصيل : يقدم الجهاز المسمى Fritzbox بموديلاته المتعددة هذه الخدمات , ويمكن الحصول عليه من المتاجر التقنية , أو من خلال الاشتراك في خدمات الانترنت , وبالطبع فإن هناك العديد من الإصدارات التي تقدم مزايا مختلفة ولكنها تشترك في النقاط التي تحدثت عنها آنفا , ولكنني اخترت الجهاز من موديل 7270 Fritzbox





المنافذ

يتمتع الجهاز بمنافذ متعددة تمكّنه من الربط مع أجهزة متعددة , وهذا ما يميزه عن راوتر الـ DSL التقليدي , الذي لا يصلح إلّا لأن يكون جهاز ربط شبكي بالانترنت , والصورة التالية توضح أهم الأجهزة التي من الممكن ربطها بالجهاز :



منافذ Ethernet + Wireless بالنسبة للتقنية التقليدية فإنّه يعمل كراوتر انترنت مع دعم لسرعات الانترنت حتى 16 ميغا بت +ADSL2 , وتوافقية مع أجهزة الشبكة من المعيار N 300 mb/s مع دعم كامل لكافة مميزات التشفير WPA2 , ودعم كامل للبروتوكول IPV6 , وكذلك بروتوكولات IPSEC-VPN , وكما هو واضح فإنه يدعم الشبكة السلكية أيضاً من خلال 4 منافذ Ethernet, وخاصية الوصول البعيد عبر الانترنت للوحة تحكم الجهاز .

منافذ RJ 11analog : وهي المنافذ التي تمكننا من توصيل أجهزة هاتف عادية بالإضافة إلى جهاز فاكس وأجهزة ISDN Phone .

منفذ ADSL : وهو منفذ يستخدم لتوصيل الراوتر مع خط الهاتف الذي يتضمن اشتراك بالانترنت .

منفذ USB : وهو منفذ يعتبر غريب بالمقارنة مع أجهزة الراوتر التقليدية , ولهذا المنفذ استعمالات هامة أهمها :

1 - كونه منفذ يمكن إدخال قرص تخزيني فيه ليتم مشاركته مع الأجهزة المتصلة بالجهاز .

2 - كونه منفذ للطابعات , من خلاله يمكن جعل الطابعة مشتركة مع الأجهزة المتصلة بالراوتر حيث أنّ هذا الجهاز يعمل Print server .

3 - في حال عدم وجود اتصال بالـ DSL يمكنك من خلال هذا المنفذ توصيل USB Stick التي تقوم بالاتصال عبر شبكات الموبايل , ومن خلال هذا الاتصال يمكنك الوصول إلى الانترنت ونشره لاسلكياً عبر هذا الراوتر .

4 - من الممكن استعمال المنفذ لتوصيل موزع شبكي ذو منفذ USB لتوسعة عدد الأجهزة السلكية الموصولة بالراوتر .

ملاحظة : يمكنك استعمال منفذ USB لتوفير ميزة مهمة وهي وضع usb wireless adaptor في هذا المنفذ لثواني , ومن ثم وضعه في جهاز الكومبيوتر , وهنا سيوفر تلقائياً وصول الكومبيوتر للراوتر دون الحاجة لإدخال إعدادات الأمان والتشفير يدوياً على الكومبيوتر , حيث أن وضع usb stick لثواني في الراوتر كفيل بنقل إعدادات الأمان إليها لتطبيقها على الكومبيوتر مباشرة !!!!

خصائص الدعم الهاتفي للجهاز

يمكن للجهاز دعم عدة أنواع من الأجهزة الهاتفية وأهمها :

1 - التلفونات العادية , وذلك مباشرة من خلال منفذ RJ11 , أو من خلال جهاز موزع مربوط بالراوتر

2 - أجهزة ISDN وأجهزة الفاكس

3 - IP telephony , وهذه الأجهزة يمكنها العمل مادمت مشتركاً مع مزودات الخدمة , ويمكنك فقط وضع الإعدادات المطلوبة داخل الراوتر وهي رقم الهاتف الذي زودك به مزود خدمة IP telephony

4 - أجهزة لاسلكية من شركة Fritzbox , وهذه الميزة تسمى DECT , وهذه الأجهزة لا تحتاج لقاعدة , فالراوتر يعمل كجهاز رئيسي وتتصل الأجهزة به لاسلكياً , ومن خلال هذه الأجهزة يمكنك إجراء الاتصالات الهاتفية بالإضافة إلى تصفح الايميل وخدمات RSS وكل ذلك مع تقنية HD , وتتم عملية الربط بين الراوتر وبين الجهاز اللاسلكي من خلال الضغط على زر DECT في الراوتر ليتم الربط مع الجهاز اللاسلكي , ويتيح هذا الموديل اتصال حتى 6 أجهزة لاسلكية .

أما بالنسبة للتحكم بالمكالمات الهاتفية كمقسم هاتفي , فإن هذا الجهاز يوفر الخدمات التالية :

- أن هذا الروتر يمكن ضبطه من خلال لوحة التحكم ليعمل كجهاز فاكس ويقوم بتحويل الفاكسات الواردة إلى أيميل معين , أو تخزينها على وحدة تخزين مثبتة بالراوتر USB flash memory
- إمكانية عمله كجهاز مجيب صوتي answering machine من خلال ملف صوتي يتم تحميله من أي جهاز متصل ويكون لديك خدمة الوصول للبريد الصوتي بعد أن تقوم بضبطها من خلال لوحة التحكم الخاصة بالجهاز .
- كما يمكنك التحكم الكامل في أوقات استقبال الهواتف وإمكانية ضبط وضع ليلي لتوقف الرنين ليلاً
- بالإضافة لإمكانية إدخال دفتر هواتف بالاسم والرقم
- بالإضافة لإمكانية حجب أو منع أرقام معينة من الاتصال , وكذلك تحويل المكالمات الواردة إلى أرقام أخرى .

وكل هذا من خلال هذا الجهاز الذي يمكن اعتبار المميزات التي يحتويها بمثابة مقسم هاتفي متكامل .

دعم الطابعات ومشاركتها

يمكنك توصيل طابعات للFritzbox من خلال منفذ USB , وبذلك تصبح الطابعة شبكية ومتاحة للأجهزة المربوطة والمتصلة على هذا الجهاز , ويتم ذلك وفقاً للخطوات التالية :

- تنصيب برنامج دعم منفذ الطابعات المحلية على جهاز الكومبيوتر ويكون موجود في القرص المرفق مع جهاز Fritzbox
- إضافة طابعة يدوياً من نافذة إضافة الطابعات في لوحة التحكم واختيار المنفذ المحلي Fritzboxusb printer port
- اختر اسم الطابعة من خلال الشركة المصنعة
- ومن ثم ضع تسمية للطابعة وبذلك تكون الطابعة أحد الطابعات الممكنة لديك , وبإمكان عدة أجهزة استخدامها ايضاً .

الاجهزة الملحقة

يمكن لمقتنيي جهاز Fritzbox الحصول على أجهزة ملحقة مفيدة وأهمها :

FRITZ!WLAN Repeater N/G

وهو جهاز يقوم بإعادة بث الشبكة اللاسلكية بالإضافة إلى أنّه يقوم ببث إشارة لمستقبلات الراديو FM لإعادة بث المحتويات الصوتية الموجودة في الـ firtzbox أو المخزنة في المجلدات المشاركة على الأجهزة المتصلة بالراوتر , وبالتالي يمكنك من خلال هذا الجهاز التحكم بالموسيقى المراد عرضها وكذلك بثها لأجهزة ستريو ملحقة .

التقنيات الملحقة

يأتي الجهاز مع سلسلة من البرامج الداعمة لعدة تقنيات حيث يأتي معه برنامج upload manager , والذي من خلاله يضيف قرص خارجي إلى جهازك يمكنك من خلاله الوصول إلى مساحة تخزين مجانية على الانترنت بسهولة وكأنه قرص موجود لديك .

وكذلك webmail manager , الذي يمكنك من التعامل مع البريد الإلكتروني بطريقة قريبة من برنامج outlook وبرنامج Easy login لتسهيل وصولك للوحة التحكم من خلال نافذة رسومية متكاملة ,

بالإضافة إلى مميزات تشغيلية وتشاركيه للملفات الموسيقية يوفرها جهاز Fritzbox .

وعلى الرغم من وجود أجهزة شبيهة في الأسواق إلّا أنّ المميزات التي يضيفها هذا الجهاز لعالم الشبكات والاتصالات و وجود كل هذه المميزات في جهاز متكامل و وجود منتجات إضافية من نفس الشركة تتكامل مع هذا الجهاز بسهولة تجعل منه جهازاً ضرورياً لكل هواة الانترنت والاتصالات المتقدمة .



تقنيات FLUKE الإحترافية في أدوات فحص الشبكات



عالم الشبكات عالماً ممتع . وبإزدياد متعة هذا العالم يزداد تعقيده . فكل يوم نرى تقنية جديدة . وكل يوم نتعرف على شيء جديد ما إذا إطلعنا. وكل يوم نواجهه مشكلة جديدة أثناء العمل على الشبكات المعقدة.

ولا شك أن كل مهندس شبكات يواجه مشاكل معقدة ويقضي الساعات لحلها .

ولكن بعد اليوم مع عالم Fluke المتخصص في أدوات الفحص الإحترافية ، سيقل تعقيد تلك المشكلات وسنتمكن من حلها في وقت أسرع وبجهود أقل.

لاشك أن للمرة الأولى تسمع عن شركة Fluke ؟؟

إنها شركة المانية تختص بأمور بتصنيع أدوات الفحص في مختلف المجالات ولها منتجات عديدة في مجالات مختلفة . إلا أننا سنتطرق لبعض أدواتها المتعلقة بمجال شبكات الحاسب الآلي ووالتي تتميز بالجودة العالية ودقة في إظهار نتائج الفحص وتعدد المهام فيها.

والآن دعنا نستعرض لكم بعض أجهزتها الإحترافية :-

جهاز AirCheck Wifi Tester

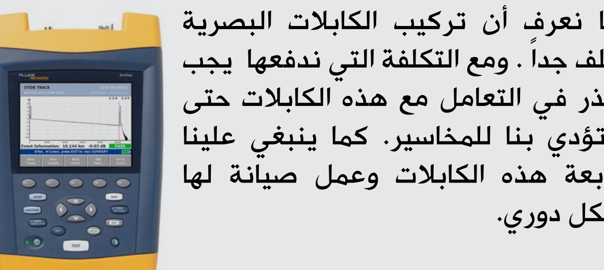


يعد هذا الجهاز أداةً إحترافية لفحص الشبكات اللاسلكية. حيث يزودك بأهم المعلومات عن الشبكات المحيطة بك. فبإستخدامه تستطيع معرفة قوة إشارة كل شبكة وترددها والقناة المستخدمة للبث والبروتوكلات التي تتعامل معها . أيضاً تستطيع معرفة الحماية المستخدمة في الشبكة ونوع التشفير.

كما يظهر لك هذا الجهاز مقارنة بين الشبكات اللاسلكية وقوة إشارة كل منها .

وتكمن فائدة هذا الجهاز عند القيام بفحص الشبكات اللاسلكية الضخمة والتي تحتوي على عشرات Access Points بحيث تستطيع معرفة قوة كل نقطة والقناة الخاصة فيها لتجاهل التشويش بين . وأيضا تستطيع معرفة النقاط ذات الإشارة الضعيفة والنقاط المتعطلة بسهولة .

جهاز OptiFiber OTDR



كما نعرف أن تركيب الكابلات البصرية مكلف جداً . ومع التكلفة التي ندفعها يجب الحذر في التعامل مع هذه الكابلات حتى لا تؤدي بنا للمخاسير. كما ينبغي علينا متابعة هذه الكابلات وعمل صيانة لها بشكل دوري.

لعمل صيانة لهذه الكابلات فإننا نحتاج لإداة إحترافية تسهل علينا العمل .
فسنستعرض جهاز Optifiber OTDR الذي يعد أحد الأجهزة القوية في هذا المجال. حيث أنه مزود بشاشة لإظهار تفاصيل الكابلات ومخططات بيانية تساعد المهندس على فحص الكابلات بدقة .
ويتميز هذا الجهاز بقدرته على تحديد موقع المشكلة في الكابل في ثوان قصيرة . كما أن له القدرة على معرفة ما إذا كانت الموصلات او الـ Connectors المثبتة على الكابل بها إن كانت موصلة بطريقة صحيحة ام بها مشكلة . أيضا يستطيع هذا الجهاز معرفة طول الكابل ونقطة بداية الفقد فيه .

ومن المميزات الرائعة في هذا الجهاز ، هو انه يتمكن من معرفة المنافذ الموصل بها الكابل اذا كانت تعمل بصورة جيدة ام بها عطل او ضعف في توصيل البيانات .

جهاز CableQ Qualification Tester

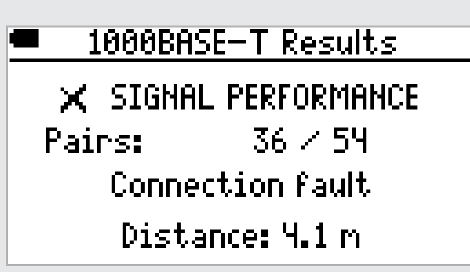


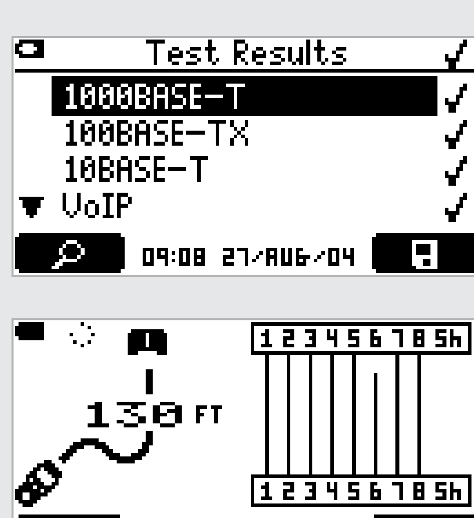
يستخدم هذا الجهاز لفحص الكابلات النحاسية مثل , Twisted Pair, Coaxial Audio Cable . ويتميز هذا الجاهز بقدرته على إكتشاف نوع الكابل وخصائصه ليعلمك ما إذا كان هذا الكيبل له القدرة لتعامل مع تقنية VoIP او Gigabyte Ethernet . كما يستطيع معرفة ما إذا كان الكابل المستخدم له القدرة على نقل كمية الـ Bandwidth المستخدم في شبكتك .

ويأتي مع هذا الجاهز ملحقات أخرى يمكن توصيلها بالطرف الاخر لمعرفة ما إذا كان الكابل موصل ام لا . وكذلك يمكن معرفة مواصفات الجهاز الموصل به الكابل مثل : Speed و Duplex .



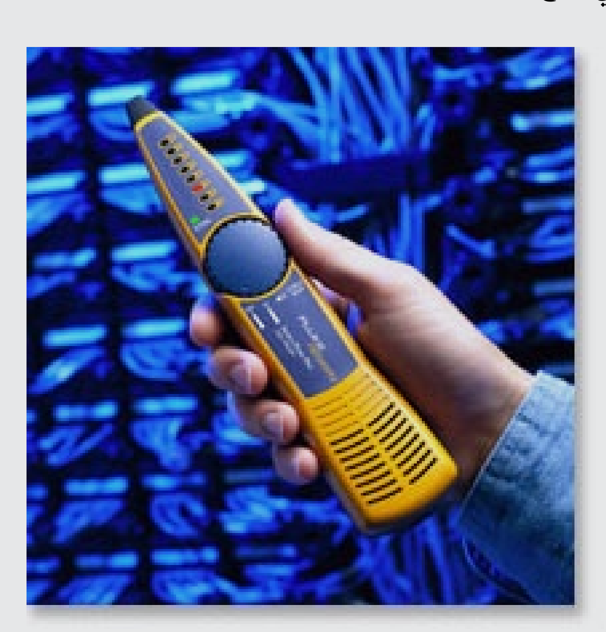
ومع وجود الشاشة الخاصة بهذا الجهاز ، تستطيع رؤية مخطط عن الكابل والأزواج الخاصة به لتتعرف أي منها منقطع او الموصل بطريقة خاطئة . كما تستطيع أيضا معرفة نوع الكابل وطوله وقوة الإشارة فيه.

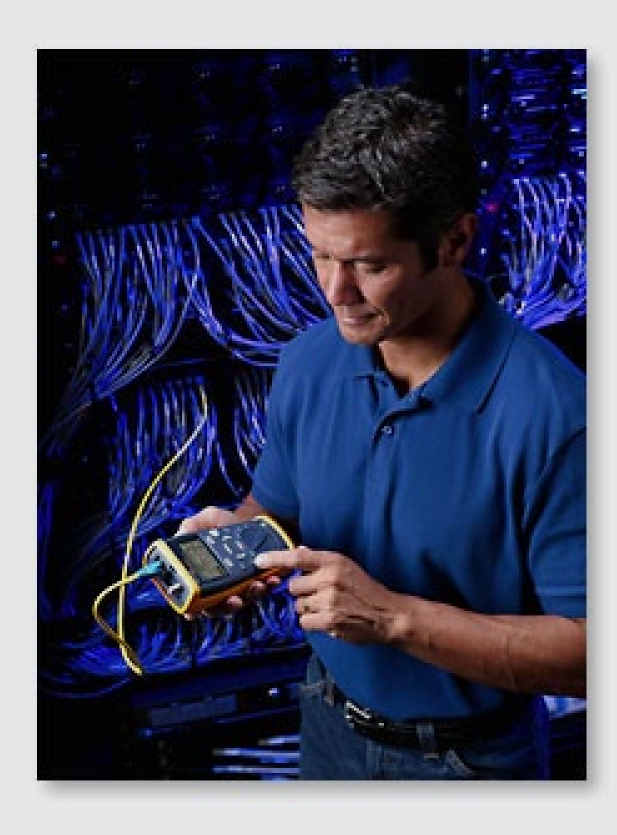




وماذا لو كنت تملك 599 كابل موصولة بـ 599 منفذ !! وتريد معرفة أي كابل والمنفذ الموصل به ؟؟

نعم تستطيع مع هذا الجهاز فتوجد أداة مرفقة معه متخصصة في تتبع الكابلات .





جهاز CableQ Qualification Tester



أما عن هذا الجاهز !! فهو التقنية الإحترافية لمراقبة الشبكات وتحليل أداء عناصرها بدقة وتفاصيل . فهو يزودك بتقرير شامل عن الشبكة ويرسله لك بشكل يومي . كما أنه يحدد لك المشكلة في ثواني معدودة .

بمجرد بدء عمل هذا الجاهز على الشبكة ، فإنه مباشرتا يبدأ بمراقبة شاملة على الشبكة. وأثناء المراقبة ، فأنه يركز على الأجهزة ذات الأداء الأقل ليرصد تقرير عنها ويرسله لمدير الشبكة .

ويتمكن هذا الجهاز أيضا من معرفة كل جهاز والـ Switch الموصل به ورقم الـ slot الخاص بذلك الـ Switch .

وعند عمل تحليل للشبكة ، فإن هذا الجهاز يقوم بتصنيف الأجهزة حسب طبيعة عملها ، مثل أجهزة VoIP وأجهزة WiFi . كما يصنف أيضا الشبكات المتفرعة حسب الـ IP Subnet .

أما عن بيئة الشبكات اللاسلكية ، فهو يقوم بالتعرف على كل Access Point والـ Clients المتصله بها . كذلك يتعرف على حماية كل Access Point وبارامترات QoS المستخدمة فيها .

ومن المميزات الجميلة فيه ، قدرته على عمل تحليل مستقل لكل شبكة VLan ومعرفة حالة الـ Trunk Ports الموجودة على الـ Switches .



Magazine

NetworkSet